Titre: Title:	Amélioration de la qualité de service dans les réseaux mobiles UMTS
Auteur: Author:	Stéphanie Boni
Date:	2006
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Boni, S. (2006). Amélioration de la qualité de service dans les réseaux mobiles UMTS [Mémoire de maîtrise, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/8380/

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/8380/
Directeurs de recherche: Advisors:	
Programme: Program:	Non spécifié

UNIVERSITÉ DE MONTRÉAL

AMÉLIORATON DE LA QUALITÉ DE SERVICE DANS LES RÉSEAUX MOBILES UMTS

STÉPHANIE BONI
DÉPARTEMENT DE GÉNIE INFORMATIQUE
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INFORMATIQUE)

FÉVRIER 2006

Your file Votre référence
ISBN: 978-0-494-47652-9
Our file Notre référence
ISBN: 978-0-494-47652-9

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

AMÉLIORATION DE LA QUALITÉ DE SERVICE DANS LES RÉSEAUX MOBILES UMTS

Présenté par : BONI Stéphanie

en vue de l'obtention du diplôme de Maîtrise ès sciences appliquées

a été dûment accepté par le jury d'examen constitué de :

M. BOUDREAULT Yves, Ph.D., président

M. PIERRE Samuel, Ph.D., directeur de recherche et membre

M. QUINTERO Alejandro, Doct., membre

À ma famille et à Junior

REMERCIEMENTS

Mes remerciements vont à l'endroit de mon directeur de recherche, le Professeur Samuel Pierre, pour son soutien et son encadrement tout au long de ma maîtrise. Je remercie aussi Yves Lemieux de Ericsson Recherche Canada pour ses conseils et le temps qu'il a consacré à me guider.

Ma gratitude va également aux membres du Laboratoire de Recherche en Réseautique et Informatique Mobile (LARIM) et plus particulièrement à Meral Shirazipour pour leurs critiques constructives lors de nos échanges sur mon sujet de recherche.

Je ne saurais oublier de dire merci à mes parents, à ma famille et à mes amis pour leurs prières et leurs encouragements. J'aimerais manifester ma reconnaissance à Paul-Marie Junior Loembé pour m'avoir poussée à entreprendre ces études de second cycle universitaire. Enfin, je rends grâce à Dieu pour sa bénédiction et son assistance lors de ce parcours.

RÉSUMÉ

Les réseaux *Universal Mobile Telecommunication System* (UMTS) offrent aux usagers des services utilisables durant leurs déplacements. À mesure que le nombre de ces usagers en déplacement augmente, il apparaît crucial de développer un support efficace de leurs communications et d'assurer ainsi une qualité de service.

En effet, les réseaux UMTS sont conçus de telle sorte que dans la majorité des cas, chaque communication d'un usager en déplacement transite par un routeur de son réseau d'origine avant d'atteindre sa destination. L'usager peut garder une référence au routeur qu'il désire pour son service grâce à l'*Access Point Name* (APN). Ce dernier possède un ancrage géographique puisqu'il pointe toujours vers le même routeur, peu importe la localisation de l'usager. De ce fait, les données subissent un détour qui induit des délais nuisant gravement à la qualité de service des communications.

L'objectif de ce mémoire est de présenter un ensemble de mécanismes permettant de réduire les délais liés à l'ancrage géographique de l'*Access Point Name* lorsqu'un usager se déplace dans un réseau UMTS autre que le sien. Ces mécanismes touchent uniquement le réseau cœur à commutation de paquets des réseaux UMTS. De plus, nous ne considérons que les cas de mobilité sans relève et la technologie d'adressage et de mobilité de la version 6 du protocole IP est utilisée.

Nous proposons de remplacer l'actuel *Access Point Name* par un identificateur de service baptisé *ServiceID*. Contrairement à l'APN qui réfère toujours au même routeur quel que soit le réseau dans lequel se trouve l'usager, le *ServiceID* fait référence au routeur capable de donner accès au réseau de données ou au service que

l'usager désire dans le réseau où il est situé. Le soin est laissé au réseau courant de l'usager de choisir le routeur approprié. Par ailleurs, puisque le *ServiceID* n'est pas un nom conforme au *Domain Name System* (DNS) mais un nombre représenté sur cinq octets, nous avons conçu différents mécanismes pour assurer la correspondance entre le *ServiceID* et l'adresse IP du routeur auquel il fait référence.

Pour évaluer notre modèle, nous avons effectué une vérification formelle avec le logiciel UPPAAL afin de nous assurer de sa fiabilité, de la cohérence de ses fonctionnalités, de la conformité du comportement du système avec nos attentes. Cette validation de protocole nous a également permis de vérifier que notre modèle possède bien les propriétés prévues dans les spécifications. Nous avons poursuivi notre évaluation de performance avec une courte analyse formelle qui a fourni une estimation de la réduction de délais occasionnée par notre modèle. Nos résultats sont plus que satisfaisants. En effet, notre modèle satisfait à toutes les exigences en matière de fonctionnalités et d'intégrité. Par ailleurs, il nous permet d'atteindre notre objectif : réduire les délais pour le trafic de l'usager en *roaming*.

ABSTRACT

Universal Mobile Telecommunication System (UMTS) networks offer services to the users while they are roaming. As the number of roaming users is growing, efficient support of this type of user's communications must be defined to ensure a certain quality of service.

Indeed, UMTS networks are conceived so that every roaming user's communication forwards by a router located in the user's home network before reaching its destination. This router manages routing and forwarding for the mobile user and the later can refer to the router he wants thanks to the Access Point Name (APN), a Domain Name System (DNS) name. The problem is the APN has a geographical dependency. That's why the APN often refers to a GGSN located in the mobile user's home network wherever he is located. Unfortunately, this geographical anchoring causes delays since data have to come back to the home network. These delays harm the UMTS networks' quality of service.

The goal of our research is to present a set of mechanisms making it possible to reduce the delays related to the geographical anchoring of the APN when a user is roaming in another network. These mechanisms only touch the packet switching domain of the UMTS core network. Furthermore, we only consider the cases of mobility whitout handover and we use the addressing and mobility technology of Internet Protocol version 6.

We propose to replace the current Access Point Name with a service identifier called *ServiceID*. Contrary to the APN that always refers to the same router wherever network the user is located in, the *ServiceID* refers to the router able to give access to the data network or the service the user wishes in the network where he is.

The care is left with the current network of the user to choose the suitable router. In addition, since the *ServiceID* is not a Domain Name System name but a five-bytes number, we designed different mechanisms to ensure the mapping between the *ServiceID* and the IP address of the router to which it refers.

To evaluate our model, we performed a formal checking with the UPPAAL software in order to ensure us of its reliability, of the coherence of its functionalities and of the conformity of its behavior with our waitings. This protocol validation allowed to us to check that our model actually has the properties envisaged in the specifications. We continued our evaluation of performance with a short formal analysis that provide us an estimate of the reduction of delays caused by our model. Our results are more than satisfactory. Indeed, our model meets all the requirements of functionalities and integrity. In addition, it enables us to achieve our goal : to reduce the delays for roaming user's traffic.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES SIGLES ET ABBRÉVIATIONS

APN	Access Point Name
AS	Autonomous System
ASN	Autonomous System Number
ATM	Asynchronous Transfer Mode
BG	Border Gateway
BGP	Border Gateway Protocol
COA	Care-of Address
CN	Correspondent Node
CTL	Computational T Language
DNS	Domain Name System
FA	Foreign Agent
FEC	Forwarding Equivalence Class
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GTP	GPRS Tunnelling Protocol
HA	Home Agent
HLR	Home Location Register
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
LEMA	Label Edge Mobility Agent

LIB	Label Information Base
LDP	Label Distribution Protocol
LER	Label Edge Router
LSP	Label Switched Path
LSR	Label Switching Router
ME	Mobile Equipment
MCC	Mobile Country Code
MIP	Mobile Internet Protocol
MNC	Mobile Network Code
MP-BGP	Multi-Protocol Border Gateway Protocol
MPLS	Multi Protocol Label Switching
MSC/VLR	Mobile Switch Center/Visitor Location Register
OSI	Open Source Initiative
OSPF	Open Shortest Path First
PDP	Packet Data Protocol
PLMN	Public Land Mobile Network
QoS	Quality of Service
RAN	Radio Access Node
RIR	Regional Internet Registries
RNC	Radio Network Controller
RSVP	Resource Reservation Protocol
RNL	Radio Network Layer
SGSN	Serving GPRS Support Node
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
UTRAN	UMTS Terrestrian Radio Access Network
VPN	Virtual Private Nerwork
VRF	VPN Routing and Forwarding

LISTE DES ANNEXES

CHAPITRE 1
INTRODUCTION

La téléphonie mobile est aujourd'hui profondément ancrée dans les habitudes de plusieurs centaines de millions de personnes dans le monde. Les réseaux qui supportent ce mode de communication évoluent pour intégrer les exigences des usagers et des fournisseurs de service. Avec le passage au numérique, la première génération (1G) de réseaux cellulaires analogiques a été remplacée par une seconde génération intégrant une meilleure qualité d'écoute et une couverture plus grande. Ces réseaux transportent principalement de la voix mais avec la demande accrue de transport de données multimédia, les réseaux de deuxième génération (2G) sont appelés à évoluer. Les réseaux *Universal Mobile Telecommunication System* (UMTS) sont des réseaux de troisième génération (3G) qui utilisent une bande de fréquences plus large pour transporter davantage de données à un débit élevé. Cependant, la mobilité intègre de plus en plus le monde du travail mais également la vie quotidienne des populations. Les réseaux UMTS doivent donc relever les défis inhérents à la gestion de cette mobilité. Ce mémoire traite de la gestion de la mobilité lorsque les usagers se déplacent dans un autre réseau que le leur.

Dans ce chapitre d'introduction, nous présentons quelques concepts et principes de base qui nous permettront par la suite d'énoncer les éléments de la problématique. Ensuite, nous précisons nos objectifs de recherche et le plan du mémoire.

1.1 Définitions et concepts de base

Les réseaux UMTS sont des réseaux de troisième génération (3G) qui, à plus ou moins long terme, remplaceront les réseaux 2G tels que le réseau *Global System for*

Mobile Communications (GSM). Néanmoins, pour faciliter la transition entre ces deux générations de réseaux, une génération intermédiaire, (2.5G), a été introduite. Il s'agit des réseaux *General Packet Radio Service* (GPRS).

Les réseaux GPRS sont divisés en deux sous-réseaux : le réseau d'accès *UMTS Terrestrial Radio Access Network* (UTRAN) et le réseau cœur. La principale fonction du réseau cœur est de fournir la commutation et le routage au trafic des usagers. En revanche, le UTRAN fournit la méthode d'accès d'interface air aux usagers mobiles.

Dans le réseau d'accès, les équipements mobiles communiquent avec les stations de bases (BS) qui sont contrôlées par des *Radio Network Controllers* (RNC). Dans le domaine à commutation de paquet du réseau cœur, les nœuds *Serving GPRS Support Node* (SGSN) gèrent la mobilité des usagers tandis que les nœuds *Gateway GPRS Support Node* (GGSN) servent de passerelle vers les réseaux de données externes comme l'Internet. Quand un usager veut envoyer des paquets en utilisant les services GPRS, il doit d'abord s'enregistrer auprès d'un SGSN puis d'un GGSN. C'est lors de l'enregistrement auprès du GGSN que l'*Access Point Name* (APN) est déterminé. L'APN fait référence au GGSN à atteindre pour rejoindre une dorsale IP externe. Par défaut, un usager tentera toujours de rejoindre un GGSN situé dans son réseau d'origine peu importe sa localisation. C'est pour cela qu'on peut dire que l'APN possède une dépendance géographique.

MPLS est une technologie qui, utilisée avec le protocole IP, remplace la recherche et l'expédition de paquets à travers le réseau basées sur l'adresse IP par les opérations plus rapides de recherche et de commutation basées sur une étiquette. Sur un segment IP/MPLS, l'en-tête IP est analysé uniquement à l'entrée et à la sortie du segment. Au point d'entrée, on assigne une classe d'équivalence (*Forwarding Equivalence Class,* FEC) au paquet et cette FEC est encodée dans un en-tête étendue du paquet sous forme d'une étiquette de longueur fixe. Aux sauts subséquents dans le segment, aucune analyse de l'en-tête IP n'est effectuée. À la place, l'étiquette est

utilisée comme index pour la recherche dans une table qui spécifie le prochain saut et la nouvelle valeur de l'étiquette. Le chemin emprunté dans un segment MPLS par un paquet appartenant à une FEC donnée est appelé un *Label Switched Path* (LSP). Les nœuds internes qui réalisent la commutation MPLS sont appelés des *Label Switching Routers* (LSR) tandis que ceux qui sont situés aux frontières sont appelés des *Label Edge Routers* (LER). De plus, la technologie est capable de fournir des services d'ingénierie de trafic, de qualité de service, de restauration de chemins pour une meilleure fiabilité ainsi que des *Virtual Private Network* (VPN).

Par ailleurs, le monde a beaucoup changé durant les dernières décennies. Au lieu de gérer des affaires locales ou régionales, de nombreuses entreprises doivent penser à une logistique et à des marchés globaux. Pour maintenir des communications rapides et sécuritaires entre tous leurs bureaux où qu'ils se trouvent, ces compagnies ont le choix entre des lignes dédiées et les *Virtual Private Network* (VPN) ou réseaux privés virtuels. Les lignes dédiées sont très coûteuses à entretenir et leurs coûts croissent avec la distance. Les VPN, en revanche, utilisent un réseau public tel que l'Internet pour relier des sites distants ou des usagers.

1.2 Éléments de la problématique

Le problème qui nous intéresse est celui de la gestion de mobilité des usagers qui passent d'un réseau UMTS à un autre. En effet, lorsqu'un usager met pour la première fois son mobile en fonction dans le réseau visité, l'équipement est inconnu du réseau en question. L'équipement mobile doit donc s'enregistrer dans le réseau visité en effectuant l'opération *GPRS attach* auprès d'un SGSN du réseau visité. Ce SGSN que nous appellerons VSGSN pour *Visited SGSN* communique alors avec le HLR (*Home Location Register*) dans le réseau d'origine du mobile afin de vérifier l'abonnement de l'usager ainsi que le droit de ce dernier de recevoir ou non des services dans un autre réseau UMTS que le sien. Si ces informations sont validées, le

VSGSN les confirme à l'équipement mobile qui peut alors lancer une procédure d'activation de *PDP context*. Cette procédure permet à l'équipement mobile d'utiliser les services GPRS en s'enregistrant auprès d'un GGSN par l'intermédiaire du SGSN qui le sert. En premier lieu, un message *Activate PDP context* est envoyé par l'équipement mobile au VSGSN qui utilise l'absence ou la présence de renseignements tels que l'*Access Point Name* (APN), le *PDP type* et la *PDP address* comme données dans le cadre d'un mécanisme de sélection de l'APN. L'APN est un nom conforme au DNS (*Domain Name System*) qui sert à identifier un GGSN. Ainsi, à la fin du mécanisme de sélection de l'APN, le VSGSN effectue une requête DNS qui aboutit soit au rejet de la demande d'activation de contexte, soit à l'obtention de l'adresse IP d'un GGSN du réseau d'origine (*Home GGSN,* HGGSN), soit à l'obtention de l'adresse IP d'un GGSN du réseau visité (*Visited GGSN,* VGGSN). Dans le cas où l'adresse d'un GGSN est obtenue, un *PDP context* est créé auprès de ce dernier qui se charge alors du routage et du transfert de toutes les données de l'équipement mobile.

Un problème se pose lorsque le mécanisme de sélection de l'APN choisit un HGGSN parce que dans ce cas de figure, les données de l'équipement doivent retourner dans le réseau d'origine avant d'être acheminées vers leur destinataire, introduisant ainsi des délais supplémentaires et intolérables lorsqu'un certain niveau de qualité de service est requis. Le défi consiste à trouver un moyen d'abolir l'ancrage dans le réseau d'origine introduit par l'APN afin de réduire les délais lorsqu'un usager visite un réseau étranger.

Cependant, les réseaux UMTS sont encore en cours de maturation et leur développement est influencé par les tendances technologiques prédites pour l'avenir. Ainsi, l'une de ses tendances préconise l'utilisation de réseaux tout-IP qui emploient les protocoles de la famille IP à tous les niveaux. Actuellement, la pile de protocoles utilisée lors du transfert de données entre les différents nœuds GSN est celle représentée à la Figure 1.1. On remarque tout de suite la redondance de la couche

IP. Afin d'éliminer cette redondance tout en suivant la tendance du tout-IP, la portion IP/GTP/IP de la pile de protocoles peut être remplacée par IP/MPLS. Ainsi le réseau de transport entre les différents nœuds GSN sera constitué d'un VPN (*Virtual Private Network*) basé MPLS. Ce dernier permettra, à l'aide d'un même ensemble d'équipements et d'infrastructures, de relier les réseaux UMTS qui partagent des ententes permettant à leurs usagers d'utiliser leurs services respectifs tout en isolant les réseaux qui n'ont aucune entente.

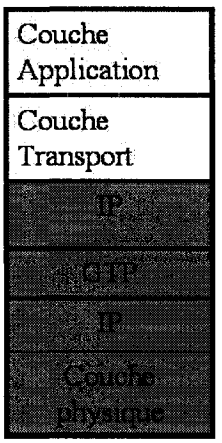


Figure 1.1 Pile de protocoles utilisée entre les nœuds GSN

Il s'agit donc de trouver un moyen d'abolir l'ancrage introduit par l'APN lorsqu'un usager visite un réseau UMTS étranger en tenant compte du réseau VPN basé MPLS qui relie les nœuds GSN.

Par ailleurs, nous nous intéressons particulièrement au réseau d'origine et le réseau visité, tous les deux situés sur des continents différents. C'est dire que ce mémoire traite d'une mobilité à grande échelle. Or, il existe dans la suite de protocoles IP, un protocole destiné à la gestion de la mobilité dans les réseaux IP : mobile IP version 6 (MIPv6). Ce protocole permet justement à un usager mobile de continuer à recevoir des données même si sa position géographique change. Dans un premier temps, l'usager choisit un routeur pouvant assumer le rôle de *Home Agent*

(HA) dans son réseau d'origine et s'y enregistre en lui communiquant sa nouvelle adresse. Par la suite, le HA intercepte tous les messages destinés à l'équipement mobile avant de les lui transmettre à sa nouvelle adresse.

MIPv6 fait partie de la version 6 de la famille de protocoles IP. Or, la version 6 du protocole IP, même si elle s'intègre peu à peu dans les réseaux, n'est pas encore supportée par tous. Ainsi, la plupart des VPNs basés MPLS supportent la version 4 du protocole IP. Il nous faudra donc trouver un moyen de résoudre ce problème de support.

Dans ce mémoire, nous traiterons donc du problème des délais introduits par l'ancrage géographique de l'APN lorsque l'usager mobile visite un réseau UMTS étranger et ce, en considérant un VPN basé MPLS comme réseau de transport entre les nœuds GSN et en faisant appel au maximum aux mécanismes du protocole MIPv6.

1.3 Objectifs de la recherche

L'objectif principal de ce mémoire est de proposer un ensemble intégré de mécanismes permettant de réduire les délais liés à l'ancrage géographique de l'APN dans un contexte de réseau visité. Pour atteindre cet objectif, nous nous attacherons à atteindre les objectifs spécifiques suivants :

- Analyser les mécanismes existants dans la littérature afin d'en déceler les forces et les faiblesses ;
- Proposer un nouveau mécanisme permettant d'abolir l'ancrage statique de l'APN dans les réseaux UMTS en utilisant la technologie d'adressage et de mobilité de la version 6 du protocole IP et en prenant en compte les cas de mobilité sans relève ;
- Valider le mécanisme proposé à l'aide d'un logiciel appropriée et évaluer ses performances par comparaison avec celles des réseaux UMTS actuels.

1.4 Plan du mémoire

Ce mémoire est composé de cinq chapitres incluant celui-ci. Le deuxième chapitre comporte une présentation générale des réseaux UMTS, de la technologie MPLS et des VPN qui l'utilisent. Le chapitre 3 présente le modèle et les algorithmes de la solution que nous proposons ainsi qu'une analyse de performance de ces derniers. Le chapitre 4 traite de l'implémentation de la solution et des résultats obtenus ainsi que de leurs comparaisons avec les valeurs à atteindre. Finalement, le chapitre 5 conclut notre mémoire avec un rappel des principaux résultats, une présentation des limites de notre solution et des indications de travaux futurs.

CHAPITRE 2
ANCRAGE DYNAMIQUE DANS LES RÉSEAUX UMTS

Le précédent chapitre nous a permis de circonscrire et définir le sujet de ce mémoire et d'en dégager la problématique : abolir l'ancrage dynamique lié à l'utilisation de l'*Access Point Name* (APN) lors de mobilité sans relève dans les réseaux UMTS. Dans ce chapitre, nous nous proposons de passer en revue les travaux les plus pertinents dans ce domaine. En premier lieu, nous abordons la gestion de mobilité dans les réseaux UMTS en mettant un accent particulier sur le rôle et l'importance de l'APN. Par la suite, nous présentons le protocole MPLS avant de nous attaquer aux VPNs (Virtual Private Networks) basés sur MPLS, et plus particulièrement, les BGP/MPLS VPNs. Finalement, nous présentons les différents mécanismes de support du protocole IPv6 et de la mobilité dans MPLS.

2.1 Gestion de mobilité dans les réseaux UMTS

Cette première section est consacrée aux réseaux de prochaine génération UMTS et, plus particulièrement, aux réseaux *General Packet Radio Service* (GPRS). Ces derniers constituent l'étape intermédiaire facilitant la transition entre les réseaux 2G *Global System for Mobile Communications* (GSM) et les réseaux UMTS.

2.1.1 Architecture de réseaux GPRS

Les réseaux GPRS sont composés de deux grandes parties :

- le réseau d'accès UTRAN (UMTS Terrestrial Radio Access Network) ;

- le réseau cœur, lui-même constitué d'un domaine à commutation de paquets et d'un domaine à commutation de circuits.

Le réseau d'accès comporte deux types d'équipements : les stations de base (BS) aussi appelées *Node B* et les RNCs (*Radio Network Controllers*). Un équipement mobile (ME) communique avec la BS la plus proche à travers l'interface sans fil *Uu*. Les paquets du ME sont découpés en *blocs de transport* puis transmis à la BS qui encapsule chaque ensemble de *blocs de transport* en une trame unique de la couche radio, RNL (*Radio Network Layer*). Cette trame est expédiée au RNC auquel la BS est rattachée à travers l'interface *Iub*.

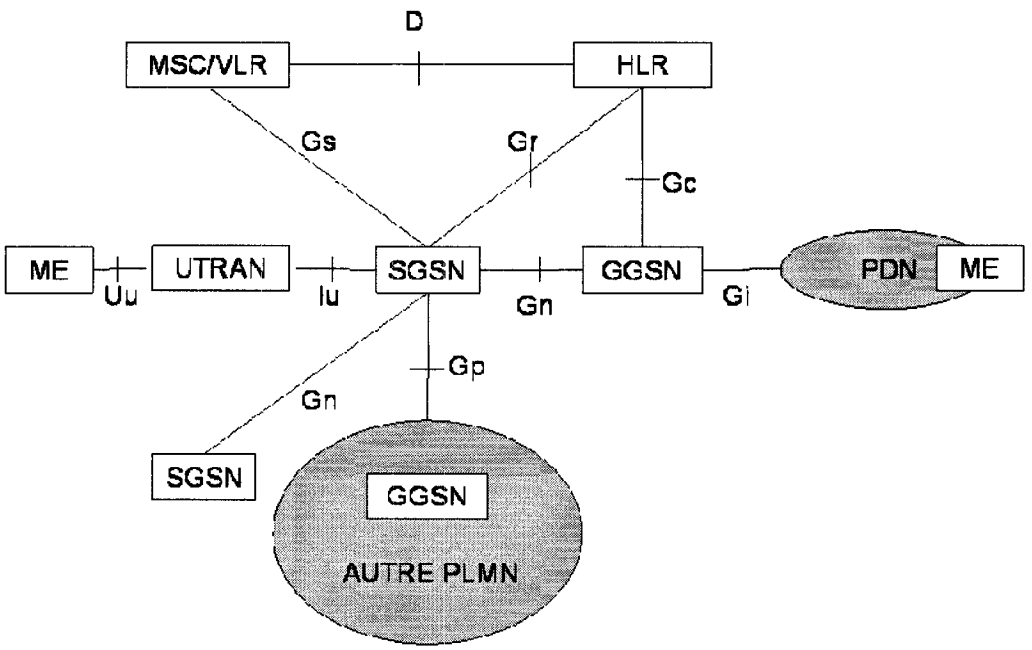


Figure 2.1 Architecture logique des réseaux GPRS

Seul le domaine à commutation de paquets (PS) du réseau cœur est d'intérêt dans ce travail. Cependant, les nœuds HLR (*Home Location Register*) et MSC/VLR (*Mobile Switch Center/Visitor Location Register*) qui font partie du domaine à commutation de circuit sont présents à la Figure 2.1 puisque nous en ferons mention plus tard.

Le domaine PS est composé de deux types de nœuds : les SGSNs (*Serving GPRS Support Node*) et les GGSNs (*Gateway GPRS Support Node*). Les SGSNs établissent différentes catégories de contextes avec le ME :

- le contexte de gestion de mobilité (*Mobility Management Context*) pour la mobilité et la sécurité du ME ; les SGSNs gèrent la mobilité inter-RNC ;
- le contexte PDP (*Packet Data Protocol Context*) utilisé conjointement avec le GGSN servant le ME pour des fins de routage et de qualité de service (QoS) ; les GGSNs s'occupent de la mobilité inter-SGSN.

Les GGSNs servent également de passerelle vers le réseau de données (PDN, *Packet Data Network*) à travers l'interface *Gi*.

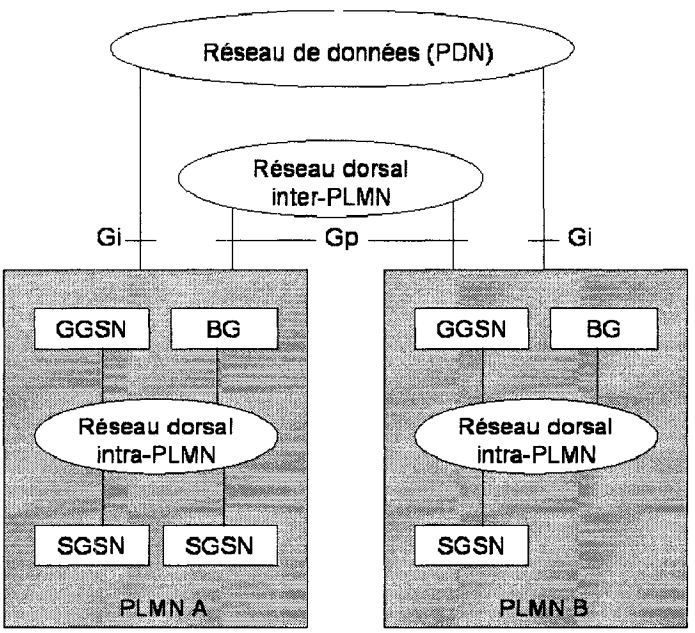


Figure 2.2 Réseaux dorsaux PLMN

Lorsqu'ils sont dans le même réseau mobile public terrestre (PLMN, *Public Land Mobile Network*), SGSN et GGSN communiquent par l'interface *Gn* tandis qu'ils utilisent l'interface *Gp* quand ils sont dans des PLMNs différents. L'interface *Gp* est une interface *Gn* mais fournit des mécanismes de sécurité supplémentaires.

La Figure 2.2 identifie les deux types de réseaux dorsaux qui interconnectent SGSN et GGSN : les réseaux dorsaux inter et intra PLMN. Un réseau dorsal PLMN est un réseau IP privé qui implémente des mécanismes de contrôle d'accès afin de garantir un certain niveau de sécurité dans le domaine PS. Deux réseaux intra-PLMN sont interconnectés via des BGs (*Border Gateways*) et un réseau inter-PLMN. Ce dernier peut être un PDN tel que l'Internet public ou encore un lien dédié.

Ce rapide survol de l'architecture des réseaux GPRS nous a permis de situer le domaine PS du réseau cœur ainsi que les réseaux dorsaux intra et inter PLMN. En effet, notre travail se focalise sur les nœuds GSNs (*GPRS Support Nodes*) et sur les réseaux qui les interconnectent. Le remplacement du protocole GTP (*GPRS Tunelling Protocol*) qui supporte la communication entre les GSNs par un réseau MPLS est préconisé dans le but d'améliorer le délai lors des relèves inter-SGSN [15]. Dans la continuité de ce travail, nous retenons l'idée de réseaux dorsaux basés MPLS mais nous ne nous intéressons pas aux relèves effectuées lorsque le ME est en mouvement. Nous étudions le scénario où un ME se retrouve dans un PLMN autre que le sien et tente de communiquer avec un autre ME.

2.1.2 Contexte PDP

Pour pouvoir accéder aux services GPRS, le ME doit d'abord effectuer l'opération *GPRS attach*. Celle-ci lui permet de créer un contexte de gestion de mobilité (*Mobility Management Context*) et de s'identifier auprès du SGSN qui le sert. Par la suite, afin de pouvoir envoyer et recevoir des paquets, le ME doit activer au moins un *PDP context* qui lui permet de s'enregistrer auprès d'un GGSN.

Un ME peut posséder un ou plusieurs *PDP Contexts*. Chaque *PDP context* contient une *PDP address*. Une même *PDP address* peut apparaître dans différents *PDP contexts*. Un *PDP context* existe soit dans l'état PDP ACTIF, soit dans l'état PDP INACTIF.

Dans ce dernier état, aucune information de routage et de mapping n'est présentée pour traiter les paquets reçus pour la *PDP Address*. Sur réception de paquets pour une *PDP Address* dont le *PDP context* est dans l'état PDP INACTIF, un GGSN peut déclencher une procédure d'activation de contexte initiée par le réseau s'il est habilité à le faire. Dans le cas contraire, des erreurs relatives à la couche réseau utilisée sont générées.

Un *PDP context* passe de l'état PDP INACTIF à l'état PDP ACTIF lorsqu'une procédure d'activation de contexte initiée soit par le ME soit par le réseau est acceptée. À l'inverse, un contexte passe de l'état PDP ACTIF à PDP INACTIF par une procédure de désactivation également initiée soit par le ME soit par le réseau. Lorsqu'il est PDP ACTIF, un *PDP context* contient toutes les informations de routage et de mapping nécessaires à la communication entre le ME et le GGSN pour la *PDP address* de ce contexte. Un ME peut aussi modifier un contexte existant.

En recevant un message *Activate PDP context request* ou un message *Activate Secondary PDP context request*, le SGSN initie les procédures d'installation de *PDP context*. La première procédure inclut les vérifications d'abonnement, la sélection de l'Access Point Name (APN) et la configuration de l'hôte, tandis que la seconde procédure exclut ces fonctions et réutilise les paramètres du *PDP context* incluant la *PDP address* mais pas les paramètres de qualité de service (QoS). Une fois activés, tous les *PDP contexts* qui partagent la même *PDP address* et le même APN sont gérés de la même façon. Au moins un *PDP context* doit être activé pour une *PDP address* pour qu'une procédure d'activation de *PDP context* secondaire soit initiée.

La procédure d'activation de contexte joue un rôle clé dans notre travail puisque c'est à ce moment que l'APN est sélectionné. L'APN est une référence à un service donné ou au GGSN à atteindre pour rejoindre le réseau externe désiré. Pour un ME en visite dans un PLMN étranger, l'APN sera une référence à un GGSN de son PLMN d'origine et c'est ici que se situe le problème.

La procédure d'activation de contexte est représentée à la Figure 2.3. Elle comporte plusieurs étapes marquées par des échanges de messages entre le ME, le SGSN et le GGSN :

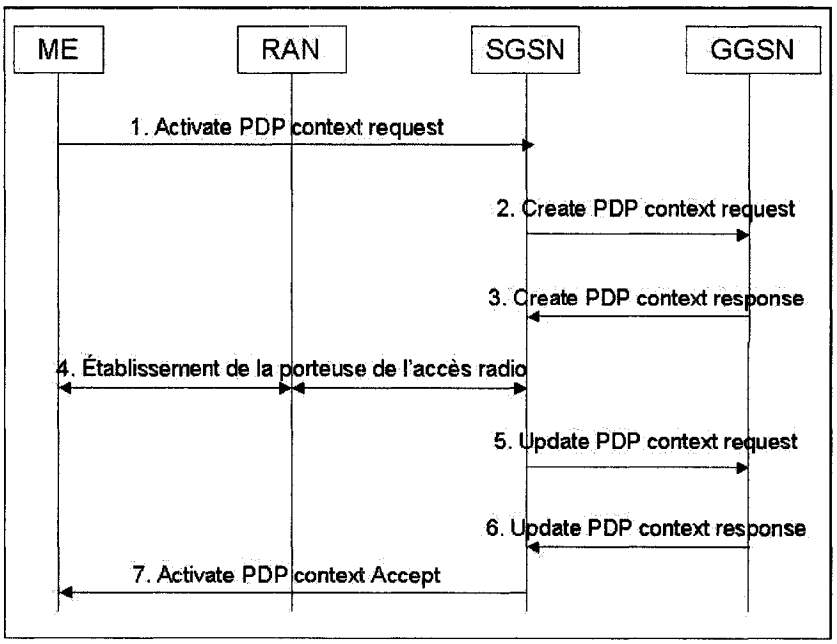


Figure 2.3 Procédure d'activation de PDP context

Étape 1 : Le ME envoie un message *Activate PDP context request* au SGSN. C'est un message de signalisation qui contient des informations clés au sujet de l'adresse IP statique de l'usager, la QoS requise pour le contexte, l'APN du réseau externe auquel la connexion est souhaitée, l'identité de l'usager et tout paramètre de configuration IP nécessaire. Sur réception de ce message, le SGSN vérifie l'enregistrement de l'abonnement de l'usager pour établir si la requête est valide. Si c'est le cas, le SGSN envoie une requête contenant l'APN à un serveur DNS (*Domain Name Server*). Le serveur DNS utilise l'APN pour déterminer l'adresse IP d'un GGSN procurant une connectivité au réseau externe désiré et retourne cette adresse IP au SGSN.

Étape 2 : Le SGSN envoie un message *Create PDP context request* au GGSN dont l'adresse a été obtenue du serveur DNS. Le GGSN crée une nouvelle entrée dans sa table de *PDP contexts* qui lui permettra de router les paquets entre le SGSN et le réseau PDN.

Étape 3 : Le GGSN retourne un message *Create PDP context response* au SGSN. Si le GGSN est responsable de l'allocation de la *PDP address*, celle-ci est incluse dans le message. Sinon, le champ correspondant est mis à 0.0.0.0 indiquant ainsi que c'est au ME de négocier une *PDP address* avec un PDN externe après la complétion de la procédure.

Étape 4 : Une procédure d'établissement de la porteuse de l'accès radio est entreprise. Elle peut entraîner une modification à la baisse de la QoS.

Étape 5 et 6 : Si les paramètres de QoS ont été modifiés, le SGSN et le GGSN échangent la paire de messages *Update PDP context request* et *Update PDP context response* afin de modifier en conséquence ces paramètres dans le *PDP context.*

Étape 7 : le SGSN envoie un message *Activate PDP context Accept* au ME pour conclure la procédure.

La procédure d'activation de *PDP context* secondaire reproduit un échange de messages similaires à celui décrit précédemment mais la réutilisation de paramètres d'un *PDP context* existant tels que la *PDP address*, l'APN allège le processus. Par ailleurs, cette procédure tout comme celle de modification de *PDP context* n'a pas d'intérêt pour nous puisqu'elle n'intervient pas sur l'APN.

Les procédures décrites ci-dessus sont initiées par le ME. Cependant, il est possible qu'elles soient initiées par le réseau par l'entremise du GGSN et dans ce cas, des messages supplémentaires allongent la procédure d'activation. En effet, le GGSN contacte le HLR (*Home Location Register*) pour déterminer le SGSN servant le ME pour lequel une activation de contexte est requise. Par la suite, le GGSN communique avec le SGSN en question qui déclenche une procédure d'activation si le ME est joignable.

2.1.3. Access Point Name

Dans un réseau dorsal GPRS, un APN est une référence à un GGSN. Pour supporter les visites inter-PLMN, une fonctionnalité de GPRS DNS interne est utilisée pour traduire un APN en adresse IP d'un GGSN.

Un APN est composée de deux parties :

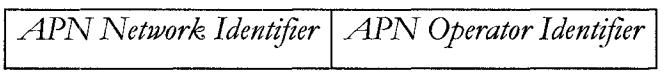


Figure 2.4 Les parties de l'APN

- l'identifiant réseau de l'APN (*APN Network Identifier*) définit à quel réseau externe le GGSN est connecté et, optionnellement, le service requis par le ME. Cette partie de l'APN doit être obligatoirement présente ;
- l'identifiant opérateur de l'APN (*APN Operator Identifier*) définit le réseau dorsal GPRS dans lequel se trouve le GGSN. Cette partie de l'APN est optionnelle.

Un APN est le nom conforme au DNS d'un GGSN d'une longueur maximale de 100 octets. Il est composé d'une ou plusieurs étiquettes ; chaque étiquette est codée comme un champ d'un octet de longueur suivi par ce nombre d'octets codé comme un caractère ASCII de 8 bits.

L'identifiant réseau d'un APN, d'une longueur maximale de 63 octets, doit comporter au moins une étiquette et il ne peut commencer par "rac", "lac", "rnc", "sgsn"; ni finir par " .gprs" et enfin il ne peut prendre la valeur "*". De plus, afin d'assurer l'unicité des identifiants réseau dans un PLMN, tout identifiant réseau de plus d'une étiquette correspond à un nom de domaine Internet alloué par le PLMN à un organisme qui a réservé ce nom. Tous les autres identifiants réseau d'APN n'ont aucune garantie d'unicité.

L'identifiant opérateur de l'APN est composé de trois étiquettes dont la dernière doit être "gprs". La première et la seconde étiquettes doivent ensemble représenter de façon unique un réseau PLMN. Chaque opérateur possède un identifiant opérateur de l'APN par défaut. Ce dernier est dérivé de l'IMSI (*International Mobile Subscriber Identity*) qui identifie de façon unique chaque usager des réseaux GPRS. On utilise plus précisément :

- le MCC (*Mobile Country Code*) composé de trois chiffres, identifiant de façon unique le pays d'origine de l'usager mobile ;
- le MNC (*Mobile Network Code*) composé de deux ou trois chiffres, identifiant le réseau PLMN d'origine du mobile.

Une forme standard de l'identifiant opérateur d'APN par défaut est la suivante :

"mcc<MCC>.mnc<MNC>.gprs"

Exemple : pour un MCC = 345, un MNC = 12, on aura l'identifiant opérateur d'APN suivant : "mcc345.mnc012.gprs".

Cet identifiant opérateur d'APN par défaut est utilisé lors des visites inter-PLMN quand est faite la traduction de l'APN (composé uniquement d'un identifiant réseau) en adresse IP d'un GGSN du PLMN d'origine. Cependant, d'autres identifiants plus faciles à comprendre pour le commun des mortels peuvent être fournis par les PLMNs.

Chaque HLR possède un champ pour stocker l'APN d'un *PDP context*. Lorsque ce champ contient un *wild card APN*, cela signifie que le SGSN peut utiliser l'identifiant opérateur d'APN reçu du mobile ou encore l'identifiant opérateur d'APN par défaut pour établir le *PDP context*. Le *wild card APN* est codé comme une unique étiquette dont la valeur "*".

Avec cette brève description de l'APN, nous achevons la présentation de la gestion de mobilité dans les réseaux UMTS. Ces réseaux sont l'objet de nombreux travaux qui traitent des différents enjeux : le *roaming* pour la voix et les données

lorsque l'usager visite un autre réseau UMTS[15] mais également le *roaming* entre des réseaux utilisant des technologies différentes[16] telles que Bluetooth et la technologie de réseaux locaux sans fil IEEE 801.11. La qualité de service dans les réseaux UMTS est également un sujet d'intérêt [17]. Ces références nous confirment que nous nous apprêtons à travailler sur un sujet intéressant au cœur des enjeux pour les réseaux UMTS.

2.2 Le protocole MPLS

Le protocole MPLS (*Multi-Protocol Label Switching*) [5] apparaît dans la littérature comme incontournable dans les réseaux IP de prochaine génération. Puisque ce mémoire traite de réseaux 3G tout-IP, nous serons donc amené à faire référence à cette technologie. Les fondements et les mécanismes du protocole MPLS feront l'objet de la section courante.

2.2.1 Les concepts MPLS

Le protocole MPLS a été créé pour répondre aux besoins accrus en vitesse et en largeur de bande que le routage traditionnel et la commutation de paquet n'ont pas su satisfaire en tenant compte des requis de qualité de service.

MPLS est le fruit du travail de l'*Internet Engineer Task Force* (IETF) et il possède différentes caractéristiques. Tout d'abord, il spécifie des mécanismes pour la gestion de flots de trafic de différentes granularités. Tout en étant indépendant des couches 2 et 3 de la pile de protocoles *Open Source Initiative* (OSI), il fait la correspondance entre les adresses IP et de simples étiquettes de longueur fixe qui sont utilisées pour expédier et commuter les paquets. MPLS possède également des interfaces pour interagir avec des protocoles de routage tels que *Open Shortest Path First* (OSPF) et *Resource Reservation Protocol* (RSVP).

La transmission de données dans la technologie MPLS est effectuée au moyen de *Label-Switched Path* (LSP), une séquence d'étiquettes établissant le chemin de nœud en nœud, de la source à la destination. Il existe deux types de LSP : les LSP *control-driven* qui sont établis avant la transmission de données et les LSP *data-driven* qui sont établis lorsqu'un flot de données est détecté. Les étiquettes sont distribuées au moyen de protocoles tels que LDP (*Label Distribution Protocol*) et RSVP ou elles sont incluses (*piggybacked*) dans des protocoles de routage comme BGP (*Border Gateway Protocol*) et OSPF. Chaque paquet encapsule et transporte les étiquettes durant son trajet entre la source et la destination et ce sont ces étiquettes qui permettent une transmission de données à haute vitesse car les équipements s'en servent pour effectuer une commutation rapide entre les liens.

2.2.2 Les composants MPLS

Les équipements qui participent aux mécanismes du protocole MPLS sont classifiés en *Label Edge Routers* (LER) et *Label Switching Routers* (LSR). Un LSR est un routeur très rapide situé dans le réseau cœur MPLS. Il participe à l'établissement des LSP au moyen de protocole de signalisation approprié avant d'effectuer la commutation des trafics de données sur ces LSP. Les LER, en revanche, sont situés en bordure du réseau d'accès et du réseau MPLS et supportent de multiples ports vers des réseaux dissimilaires tels que l'*Asynchronous Transfer Mode* (ATM) ou l'Ethernet. Les LER jouent un rôle important dans la création et la destruction des étiquettes puisque le trafic entre et sort par eux.

Une *Forward Equivalence Class* (FEC) ou classe d'équivalence est une représentation d'un groupe de paquets qui partagent les mêmes requis durant leur transport. Tous les paquets appartenant à ce groupe sont donc traités de la même manière sur leur chemin jusqu'à destination. L'assignation d'un paquet à une FEC est

faite uniquement lorsque le paquet entre dans le réseau. Chaque LSR bâtit une table *Label Information Base* (LIB) contenant les correspondances FEC-étiquette.

Les étiquettes utilisées par un LSR pour la correspondance FEC-étiquette sont divisées en deux catégories :

- Par plate-forme : les étiquettes sont uniques dans le LSR ;
- Par interface : les étiquettes distribuées sur plusieurs interfaces différentes peuvent être les mêmes.

Une étiquette dans sa forme la plus simple identifie le chemin que doit emprunter un paquet. Le routeur qui reçoit le paquet examine l'étiquette afin de déterminer le prochain saut. Les étiquettes ont une signification locale uniquement, c'est dire qu'elles ne sont pertinentes qu'entre deux LSR. Chaque paquet peut posséder une ou plusieurs étiquettes qui forment une pile. Le format général d'une étiquette est présenté au tableau ci-après.

Tableau 2.1 Format général d'une étiquette MPLS

Étiquette	Exp	S	TTL
20 bits	3 bits	1 bit	8 bits

Le champ *Exp* (usage expérimental) est utilisé comme indicateur de priorité tandis que le champ *S* indique si l'étiquette se trouve ou non au bas de la pile d'étiquettes MPLS. Enfin, le champ TTL sert à éviter des boucles infinies dans le réseau en limitant la durée de vie des paquets. Ce groupe de champs peut former l'en-tête shim MPLS, qui s'insère entre les en-têtes des couches liaison et réseau, comme il peut être incorporé dans un en-tête de la couche liaison.

MPLS fournit deux options pour l'établissement des LSP :

- le routage saut par saut : chaque LSR choisit indépendamment le prochain saut pour une FEC donnée ;

- le routage explicite : le LSR en amont spécifie une liste de nœuds par lesquels le LSP doit absolument passer. Le long du chemin, les ressources doivent être réservées pour assurer la qualité de service du trafic de données.

Tout LSP établi pour une FEC est unidirectionnel par nature. Le trafic en sens inverse doit emprunter un autre LSP.

Le survol du protocole MPLS effectué dans cette section a fourni une description non exhaustive des équipements, concepts et opérations qui entrent dans la mise en œuvre de cette technologie. Nous avons ainsi posé les bases afin de pouvoir poursuivre notre investigation.

2.3 Les VPNs basés sur MPLS

Un *Virtual Private Network* (VPN) ou réseau privé virtuel est un ensemble de sites communiquant entre eux mais également un ensemble de politiques contrôlant la connectivité et la qualité de service entre ces sites. Un réseau VPN est privé parce qu'il est à l'usage exclusif d'une compagnie ou d'une organisation et que son plan d'adressage et de routage est indépendant des autres réseaux. Un VPN est virtuel parce qu'en pratique, il partage ses ressources avec d'autres réseaux.

Dans cette section, nous nous intéressons plus particulièrement aux VPNs basés MPLS [20]. En effet, ce travail utilise des réseaux UMTS dans lesquels les nœuds GSN ne communiquent plus grâce au protocole GTP (*GPRS Tunelling Protocol*) mais plutôt à travers un VPN basé MPLS.

2.3.1 Les types de VPNs basés MPLS

Il existe essentiellement deux modèles de VPNs basés MPLS :

- le modèle de recouvrement (*Overlay Model*) ;
- le modèle pair (*Peer Model*).

Le modèle de recouvrement est le plus répandu. Dans ce dernier, chaque site d'un VPN possède un routeur qui est relié par des liaisons point-à-point à chacun des routeurs des autres sites. La complexité de tels réseaux augmente vite avec le nombre de sites. Il en résulte que les VPNs conçus selon le modèle de recouvrement ont une évolutivité limitée. De plus, un fournisseur de services doit maintenir un réseau avec des infrastructures séparées pour chaque VPN client : ce qui limite sévèrement le nombre de clients qu'il peut avoir et majore le coût des services.

Le modèle pair, en revanche, est conçu pour palier les lacunes du modèle de recouvrement. Dans ce modèle, les routeurs des différents sites ne sont plus reliés point à point comme dans le précédent. Cela le rend plus flexible pour permettre d'interconnecter non pas uniquement les sites d'un usager mais aussi les réseaux de différents fournisseurs de service [21]. Pour décrire ce modèle, nous utiliserons l'une de ses implémentations : BGP/MPLS VPN.

2.3.2 BGP/MPLS VPN

Le BGP/MPLS VPN [4] constitue notre choix de VPNs basés MPLS pour la communication entre les nœuds GSN. Avant d'en exposer les principales caractéristiques, décrivons les éléments qui le composent. La Figure 2.5 présente un exemple de BGP/MPLS VPN dans lequel les sites de deux VPNs A et B sont reliés par l'intermédiaire d'un fournisseur de service. Un site de VPN est relié au fournisseur par un ou plusieurs *Customer Edge Routers* (CE). Ainsi, le site 1 du VPN A possède un *Custormer Edge Router* CE_{A1}, tandis que le site 1 du VPN B en possède deux, $CE_{B1}{}^{1}$ et $CE_{B1}{}^{2}$. Du coté du fournisseur de service, le CE est relié à un *Provider Edge Router* (PE) et ce dernier peut être connecté à des CEs de différents VPNs. De plus, les sites de ces VPNs peuvent utiliser les mêmes adresses IP. Prenons l'exemple du *Porvider Edge Router* PE_2 qui est relié à CE_{A2} et CE_{B2} dont les adresses IP utilisées sont 10.2/16. Enfin, nous avons les *Provider Routers* (P) qui relient les PEs entre eux.

À présent, intéressons-nous aux caractéristiques des BGP/MPLS VPN. Il en existe trois, si on exclut l'utilisation de la technologie MPLS :

- Les multiples tables d'expédition ;
- Les attributs de communauté étendue de BGP ;
- les adresses VPN-IP.

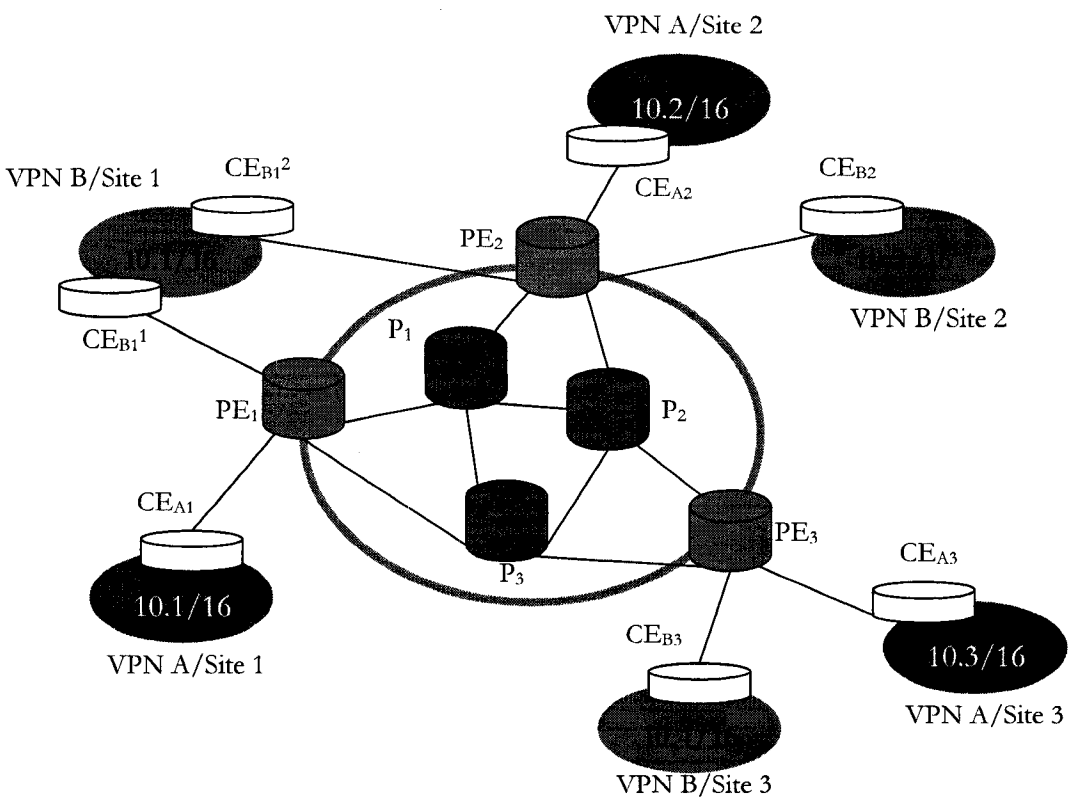


Figure 2.5 Exemple de BGP/MPLS VPN

Rappelons qu'un VPN est un ensemble de politiques qui contrôlent la connectivité entre les sites. Dans le modèle BGP/MPLS VPN, ce contrôle est accompli en contraignant le flot des informations de routage. En effet, puisque le flot de données est contrôlé par les tables de routage, la distribution contrainte des

informations de routage limite les destinations possibles afin de relier les sites tel qu'on le désire. Cette connectivité restreinte est réalisée grâce aux multiples tables d'expédition et aux attributs de communauté étendue de BGP.

En effet, chaque routeur PE maintient une ou plusieurs tables *VPN Routing and Forwarding* (VRF) par site. Ces dernières contiennent les routes pour tous les VPNs dont le site est membre. Un routeur PE détermine quelle table VRF utiliser d'après la sous-interface d'entrée du paquet. Le routeur PE peuple une table VRF en recevant les routes du CE et des PEs connectés aux VPNs dont le site est membre en utilisant les attributs de communautés étendue de BGP. Cette utilisation de plusieurs tables d'expédition au sein d'un même PE permet d'éviter la communication entre sites sans VPN en commun et de réduire la taille des tables VRF au strict minimum, facilitant ainsi l'évolutivité.

Les attributs de communauté étendue de BGP, en revanche, sont utilisés pour filtrer les routes lors de leur importation ou de leur exportation dans les messages BGP. Chaque communauté étendue doit être globalement unique et peut être utilisée par un seul VPN. Le filtrage de route a lieu à deux endroits : au routeur PE en amont qui attache l'attribut de communauté appropriée à la route qu'il exporte et au routeur PE en aval qui utilise l'attribut des différentes routes pour les importer ou non. L'utilisation des attributs de communauté étendue a un effet notable sur l'évolutivité. En effet, un routeur CE ne maintient des "relations de routage" qu'avec le routeur PE auquel il est connecté et non avec tous les autres CEs de son VPN, comme dans le modèle de recouvrement. De plus, les routeurs PEs n'entretiennent que les routes pour les sites auxquels le routeur CE est connecté.

Jusqu'à présent, nous avons décrit les mécanismes permettant de restreindre la connectivité entre les sites par VPN. Cependant, ces mécanismes utilisent BGP qui assume que les adresses IP sont globalement uniques. Cette supposition est incorrecte puisque dans l'environnement d'un fournisseur de service VPN, plusieurs VPN peuvent utiliser le même espace d'adressage. Aussi, pour résoudre ce problème

de recouvrement d'espace d'adressage, un nouveau type d'adresse a été inventé : les adresses VPN-IP.

2.3.3 Les adresses VPN-IP

Une adresse VPN-IP est construite en concaténant un *route-distinguisher* (RD) à une adresse IP. Le *route-distinguisher* est l'élément qui rend globalement unique chaque adresse VPN-IP. Il est structuré de façon à ce que chaque fournisseur de services VPN puisse créer ses RDs sans risque de duplicata. Le Tableau 2.2 présente la structure d'un RD composé de trois champs. Le champ *Autonomous System Number* (ASN) contient l'ASN du fournisseur de services VPN tandis le champ *Assigned Number* est contrôlé par le fournisseur de services qui l'utilise à sa discrétion. Généralement, un numéro est assigné au VPN.

Tableau 2.2 Structure d'un *route-distinguisher*

Route-distinguisher de 8 octets		
Type	Autonomous System Number (ASN)	Assigned Number
2 octets	2 octets	4 octets

Le protocole *MultiProtocol BGP* (MP-BGP) est utilisé et non simplement BGP. Il peut traiter de multiples familles d'adresses : il en résulte qu'aucun mécanisme supplémentaire ne doit être introduit pour l'utilisation des VPN-IP.

De plus, l'utilisation des adresses VPN-IP est confinée à l'intérieur du réseau du fournisseur de services. Chaque routeur PE est configuré de façon à déterminer le VPN d'une route à partir de son interface d'entrée. Par la suite, il exporte cette route après avoir converti ses informations d'adresse IP à VPN-IP avec le RD approprié. Il faut souligner que ni le RD, ni la communauté BGP n'identifie un VPN. En effet, un VPN peut utiliser plusieurs RDs et différents attributs de communauté étendue.

Par ailleurs, les adresses VPN-IP ne sont pas transportées dans les en-têtes des paquets IP mais dans les protocoles de routage (BGP). Le transport des paquets est assuré par MPLS qui découple les informations utilisées pour l'expédition des paquets (les étiquettes) des informations transportées par les en-têtes IP. Il s'ensuit que seuls les routeurs PE et P doivent supporter le protocole MPLS. Les routeurs PEs qui assurent le rôle de *Label Edge Router* (LER) s'occupent d'établir la correspondance entre les *Label Switch Paths* (LSP) et les adresses VPN-IP. La pile de deux étiquettes permet aux routeurs P, qui jouent le rôle de *Label Switch Router* (LSR), de ne garder aucune information de routage VPN.

Dans cette section, nous avons décrit les particularités des réseaux VPNs basés MPLS et plus précisément des VPNs BGP/MPLS. Ces derniers utilisent le protocole BGP et ses extensions pour la distribution des informations de routage et le protocole MPLS pour l'expédition des paquets. Cette dernière est basée sur un nouveau type d'adresses, les adresses VPN-IP qui permettent de garantir l'unicité des adresses à travers tous les VPNs gérés par un ou plusieurs fournisseurs de services.

2.4 Support du protocole IPv6 dans les réseaux MPLS

La section précédente nous a permis de présenter le type de réseaux de transport utilisé pour la communication entre les différents nœuds GSN du réseau cœur UMTS. L'utilisation des VPNs BGP/MPLS permet en effet de simplifier la pile de protocoles utilisée par les nœuds GSN en remplaçant la redondance IP/GTP/IP par IP/MPLS. Néanmoins, il est important de souligner que les réseaux MPLS actuels, bien que supposés indépendants des protocoles de couche 2 et 3, sont fortement reliés aux réseaux IPv4. Or l'une des principales caractéristiques de ce travail est d'utiliser la version 6 du protocole IP. Cette section a donc pour but de décrire les mécanismes permettant aux réseaux MPLS de supporter le protocole IPv6.

2.4.1 Les différentes stratégies

En ce qui concerne les mécanismes de support du protocole IPv6 dans les réseaux MPLS, il en existe plusieurs déjà disponibles et d'autres sont encore en cours de développement. Différentes stratégies sont adoptées selon qu'on se trouve dans la phase d'intégration, durant laquelle les versions 4 et 6 du protocole IP coexistent, ou dans la phase finale du processus dont le but est de remplacer IPv4 par IPv6. Trois modèles possibles de support d'IPv6 dans MPLS sont cités [12]:

- Le premier préconise d'étendre les fonctionnalités des seuls routeurs de bordure, les LERs (*Label Edge Routers*) ;
- Le second étend les fonctionnalités IPv6 aux protocoles de signalisation et de routage : cette extension touche tous les LSRs (*Label Switch Routers*) qu'ils soient en bordure ou non ;
- Le dernier, quant à lui, utilise le protocole IPv6 dans tous les aspects de la gestion des réseaux MPLS.

Ces modèles incarnent différentes étapes dans le processus d'intégration du protocole IPv6 et ils ne sont pas exclusifs. Le premier modèle correspond à la phase initiale d'intégration dans laquelle on veut introduire le nouveau protocole sans nuire aux performances du protocole déjà installé. Le second modèle décrit une situation dans laquelle l'intégration est plus avancée : le nombre d'utilisateurs du nouveau protocole n'est plus minoritaire. Enfin, le troisième modèle décrit le but ultime de l'intégration. Ces trois modèles peuvent bien sûr coexister et être introduits étape par étape.

Toute une variété de stratégies de support IPv6 dans MPLS existent [10]. La première laisse intact le réseau MPLS et n'affecte que les *Customer Edge routers* (CE) qui encapsulent les paquets IPv6 dans des paquets IPv4. Une autre stratégie consiste à "tunneler" le trafic IPv6 en utilisant n'importe quel transport sur MPLS de la

couche 2 tels que ATM sur MPLS ou Ethernet sur MPLS. Cette dernière stratégie, encore une fois, ne modifie en rien le réseau MPLS lui-même. Les auteurs poursuivent avec une stratégie correspondant au premier modèle [12] : les LERs ou *Provider Edge routers* (PE) aux fonctionnalités étendues sont rebaptisés 6PEs. Il est également possible d'ajouter une fonctionnalité VPN aux routeurs 6PEs. Ils deviennent alors des routeurs 6VPEs. Ces deux types de routeurs sont décrits dans la prochaine section.

Une autre section est consacrée à un mécanisme de support complètement différent des précédents : *IP next generation Label Switching* ou IPngLS utilisant le *flow label* de l'en-tête IPv6.

2.4.2 L'utilisation du *flow label* de l'en-tête IPv6

Actuellement, la commutation d'étiquettes est utilisée uniquement dans le protocole MPLS. Ce dernier ajoute un en-tête entre les en-têtes de couche 2 et 3 des paquets IPv4 : l'en-tête shim. La partie principale de cet en-tête shim, représenté par le Tableau 2.3, est l'étiquette permettant de déterminer l'interface de sortie du paquet et la valeur de la nouvelle étiquette. Le champ *Exp* (usage expérimental) est utilisé comme indicateur de priorité tandis que le champ *S* indique si l'étiquette se trouve ou non au bas de la pile d'étiquettes MPLS. Enfin, le champ TTL sert à éviter des boucles infinies dans le réseau en limitant la durée de vie des paquets.

Tableau 2.3 En-tête shim

Étiquette	Exp	S	TTL
20 bits	3 bits	1 bit	8 bits

Le Tableau 2.4 décrit les différents champs présents dans un en-tête de paquets IPv6. On retrouve entre autres le champ *flow label* de 20 bits dont l'usage n'est pas clairement établi dans la littérature.

L'idée maîtresse de la technologie IPngLS (*IP next generation Label Switching*) est l'utilisation du champ *flow label* de l'en-tête IPv6 pour accueillir l'étiquette MPLS de 20 bits [11]. Aucune conversion n'est nécessaire puisque les deux champs possèdent la même taille. Par ailleurs, cette technique contribuera à diminuer la complexité de la pile de protocoles en supprimant l'en-tête shim. De plus, aucun mécanisme supplémentaire ne devra être implémenté pour supporter la qualité de service, puisque IPv6 est compatible avec le protocole DiffServ (*Differentiated Services*). Néanmoins, il faut souligner que cette technique n'est applicable que dans les réseaux IPv6 : les paquets IPv4 ne peuvent être supportés.

Tableau 2.4 En-tête IPv6

Version (4 bits)	*Traffic Class* (8 bits)	*Flow label* (20 bits)	
Payload length (16 bits)		*Next Header* (8 bits)	*Hop Limit* (8 bits)
Adresse source (128 bits)			
Adresse destination (128 bits)			

Dans cette section, nous avons examiné les différentes stratégies de support du protocole IPv6 dans les réseaux MPLS. Deux techniques ont retenu notre attention : la technologie des routeurs 6PEs et 6VPEs et l'utilisation du *flow label* de l'en-tête des paquets IPv6. La première technique permet une coexistence des protocoles IPv4 et IPv6 tout en ayant un impact minimal sur le réseau dorsal MPLS. La seconde technique est exclusive au protocole IPv6 mais a l'avantage de supprimer les quatre octets de l'en-tête shim sans nuire à la performance de la commutation d'étiquette.

Cependant, la technologie des routeurs 6PEs et 6VPEs est plus attrayante car elle constitue en quelque sorte une extension du modèle VPN BGP/MPLS.

2.5 Le protocole Mobile IPv6

Avant d'aborder le sujet du support de la mobilité dans le protocole MPLS, intéressons-nous à la mobilité dans le protocole IPv6. Cela permettra de faire la transistion entre ces deux sections.

Le protocole MIPv6 [7] permet aux noeuds de rester joignables pendant qu'ils se déplacent dans un réseau Internet IPv6. Chaque nœud mobile (MN) est identifié par sa *Home Address* peu importe son point d'attachement au réseau Internet. Lorsqu'il n'est pas situé dans son réseau domicile, un MN possède également une *Care-of Address* qui fournit des informations sur la position courante du MN. Des paquets IPv6 adressées à la *Home Adress* du MN sont routés de façon transparente à la *Care-of Address* du MN. Le protocole permet aussi aux nœuds IPv6 de sauvegarder une correspondance entre la *Home Address* et la *Care-of Address* d'un MN et d'envoyer les paquets de ce dernier directement à sa *Care-of Address.*

Une *Care-of Address* est une adresse IPv6 associée à un MN et qui a le préfixe de sous-réseau d'un lien étranger particulier.
L'association entre la *Home Address* et la *Care-of Address* d'un MN est appelée un *binding* pour ce MN. Tant qu'il est loin de son réseau domicile, le MN enregistre sa *Care-of Address* primaire auprès d'un routeur de son lien domicile qui joue le rôle de *Home Agent.* Le MN accomplit l'enregistrement de ce *binding* en envoyant un message *Binding Update* au *Home Agent.* Ce dernier répond par un message *Binding Acknowledgement.*

Un nœud qui communique avec un MN est appelé un nœud correspondant (CN) et peut être stationnaire ou mobile. Il existe deux modes de communication entre le MN et le CN :

- Le tunnelage bidirectionnel
- L'optimisation de route

Le tunnelage bidirectionnel ne requiert pas que le CN supporte MIPv6 et il est disponible même si le MN n'a pas enregistré son *binding* courant auprès du CN. Les paquets du CN sont routés jusqu'au *Home Agent* puis tunnelés au MN. Les paquets pour le CN sont tunnelés depuis le MN jusqu'à son réseau domicile avant d'être routés normalement jusqu'au CN.

L'optimisation de route nécessite que le MN enregistre son *binding* courant auprès du CN. Les paquets provenant du CN peuvent être routés directement à la *Care-of Address* du MN. Lorsqu'il envoie un paquet vers n'importe quelle destination IPv6, le CN vérifie d'abord parmi ses *bindings* sauvegardés s'il ne possède pas une entrée pour l'adresse de destination du paquet. Si une entrée existe, le CN utilise un nouveau type d'en-tête de routage IPv6 (*Mobility Header*) pour router le paquet jusqu'au CN grâce à sa *Care-of Address*.

Il existe également un mécanisme permettant au MN de découvrir les adresses des routeurs agissant comme *Home Agent* dans son réseau domicile : *Dynamic home agent address discovery*.

La *Mobility Header* ou en-tête de mobilité est une extension d'en-tête utilisée par les MN, CN et les *Home Agents* pour créer et gérer les *bindings*. La *mobility Header* est identifiée par la valeur 135 dans le champ *Next Header* de l'en-tête qui la précède directement.

Tableau 2.5 Format de la *Mobility Header*

Payload Proto	Header Len	MH type	Reserved
Checksum			
Message Data			

- Payload Proto : sélecteur de 8 bits qui identifie le type d'en-tête qui suit immédiatement la *Mobility Header.* (même valeur que le champ *Next Header* de IPv6) ;
- Header Len : entier non signé représentant la longueur de la *Mobility Header* en unité de 8 octets et excluant les 8 premiers octets. La longueur de l'en-tête doit être un multiple de 8 octets ;
- MH type : sélecteur de 8 bits qui identifie le type de message en question. Un type inconnu provoque une indication d'erreur ;
- Reserved : réservé pour usage futur ;
- Checksum : entier non signé de 16 bits contenant la *checksum* de la *Mobility Header* ;
- Message Data : champ de longueur variable contenant les données spécifiques du type de message spécifié par le MH type.

MIPv6 définit également un certain nombre de *Mobility Options* à utiliser dans ses messages. Si elles sont incluses, ces options doivent apparaître après la portion fixe du champ *Message Data.* La présence de telles options est indiquée par le champ *Header Len* dans le message. Quand la valeur du champ *Header Len* est plus grande que la longueur requise pour le type de message spécifié, les octets restants sont interprétés comme des options.

L'option *Home Address* est transportée dans l'en-tête d'extension *Destination Option* (valeur du champ *Next field* = 60). Cette option est utilisée par le MN lorsqu'il est loin de son réseau domicile pour informer le destinataire de sa *Home Address.*

L'en-tête de routage de type 2 *(Type 2 routing header)* permet le routage des paquets directement du CN à la *Care-of Address* du MN. La *Care-of Address* du MN est insérée dans le champ *Destination Address.* Une fois le paquet arrivé à la *Care-of Address*, le MN retrouve sa *Home Address* dans l'en-tête de routage et celle-ci est utilisée comme adresse de destination finale pour le paquet.

La nouvelle en-tête de routage utilise un type différent de celui du routage de source régulier IPv6. Elle permet aux pare-feux d'appliquer des règles différentes aux paquets utilisant le même routage de source que MIPv6.

Nous achèverons cette section en rappelant que les technologies reliées à IPv6 comme MIPv6, sont en cours de déploiement. Différentes stratégies existent pour accomplir ce déploiement mais aussi pour assurer la coexistence avec la technologie IPv4 [22].

2.6 Support de la mobilité dans MPLS

Dans la section précédente, nous avons brièvement décrit le protocole Mobile IPv6. La technologie IP est pressentie pour être la base des réseaux mobiles de prochaines générations [23]. Dans cette section, nous examinons comment MPLS, une technologie IP, peut supporter la mobilité des usagers. Deux mécanismes sont présentés : la technologie MPLS mobile et la micro mobilité basée MPLS.

2.6.1 MPLS mobile

Le protocole MPLS mobile intègre la mobilité IPv4 et le protocole MPLS afin que ce dernier puisse supporter la mobilité [13]. Tout d'abord, lorsqu'un usager mobile pénètre dans un réseau étranger, il envoie un message *Registration Request* au *Foreign Agent* (FA) du réseau. Ce dernier relaie le message contenant l'adresse *care-of* (COA) de l'usager mobile au *Home Agent* (HA) de celui-ci. Fort de cette information, le HA peut alors négocier l'établissement d'un *Label Switched Path* (LSP) entre le FA et lui avec la COA de l'usager mobile comme *Forwarding Equivalent Class* (FEC).

Ainsi, lorsqu'un nœud correspondant (*Correspondent Node*, CN) voudra communiquer avec l'usager mobile, les paquets seront interceptés par le HA. Puis, ce dernier utilisera l'étiquette des paquets entrants pour déterminer dans sa table d'étiquettes la nouvelle étiquette à apposer et le port de sortie. Les paquets seront

donc délivrés du HA au FA par l'intermédiaire du LSP établi précédemment. Ensuite, le FA transmettra les paquets à l'usager mobile par routage IP.

Le mode opératoire que nous venons de décrire correspond à la version basique du protocole MPLS mobile, celle sans optimisation de route (*Route Optimization*). Les paquets expédiés par le CN à l'usager mobile transitent par le réseau d'origine du destinataire avant de rejoindre celui-ci. Il s'agit du problème de routage triangulaire (*Triangle routing*) puisque les paquets ne suivent pas le chemin optimal entre la source et la destination. Une extension de MPLS mobile permet de solutionner ce problème : MPLS mobile avec optimisation de route.

Avec cette extension du protocole, le CN peut sauvegarder une entrée pour l'usager mobile et établir un LSP directement avec ce dernier en se servant de sa COA. Les paquets sont alors expédiés à l'usager mobile sans passer par le HA. Néanmoins, au début de la communication, le mode opératoire de MPLS mobile sans optimisation de route est utilisé puisque le CN n'a aucune entrée pour l'usager mobile. En recevant les paquets du CN, le HA déduit que ce dernier ne possède pas d'entrée pour l'usager mobile. Le HA fait suivre les paquets via le LSP entre le FA et lui et envoie un message *Binding Update* au CN pour l'informer de la COA de l'usager mobile. Le CN peut alors établir le LSP avec l'usager mobile.

Cette version avec optimisation de route apporte une solution au problème de routage triangulaire qui peut engendrer des délais supplémentaires. Cependant, les premiers paquets expédiés continuent à transiter par le réseau d'origine. Pour certaines applications sensibles aux délais, les premiers paquets servent à l'initialisation et à l'établissement des connections. Les délais dus au routage triangulaire peuvent se révéler inacceptables pour ces applications.

2.6.2 Micro mobilité basée MPLS

Dans un réseau tout-IP de troisième génération, il existe trois niveaux de mobilité [14]:

- La mobilité d'accès aussi appelée mobilité de couche liaison. Elle fait référence aux protocoles et méthodes assurant une communication ininterrompue entre un usager mobile en mouvement et les stations de base (*Base Stations*, BS) gérés par un même RNC (*Radio Network Controller*) ;
- La mobilité à grande échelle : ce type de mobilité est géré par la famille de protocoles mobilité IP et fait référence aux mouvements de l'usager mobile entre différents nœuds GSN (*GPRS Serving Node*) ;
- La micro mobilité : il est possible d'étendre le concept de mobilité à grande échelle aux nœuds RNC. Cependant, puisque les changements de RNCs interviennent plus souvent que les changements de GSNs, il en résulte une surcharge de signalisation et une grande latence dans le support de la mobilité. La micro mobilité est un mécanisme plus léger permettant de gérer ce type de mobilité.

Différents protocoles existent pour gérer la micro mobilité. Ils sont divisés en deux grands groupes en fonction du mécanisme utilisé : le routage et les tunnels. Dans la catégorie des protocoles utilisant le routage, on range les protocoles Hawaï et IP cellulaire (*Cellular IP*). L'enregistrement régional (*Regional Registration*) et HMIPv6 (*Hierarchical Mobile IP version 6*) forme la catégorie des protocoles utilisant les tunnels.

Le schéma de micro mobilité basée MPLS [14] recycle les principes des schémas utilisant les tunnels et plus particulièrement HMIPv6. Ils définissent une fonction de *Label Edge Mobility Agent* (LEMA). En premier lieu, un nœud fonctionnant comme LEMA agit comme un LER standard et fait la correspondance entre une adresse IP de destination d'un paquet et une FEC. La FEC elle-même est

non seulement associée à une paire contenant l'identité du prochain saut et la nouvelle étiquette MPLS, mais elle identifie également un LSP. En second lieu, un nœud agissant comme LEMA crée pour une adresse IP donnée une nouvelle correspondance avec une FEC en réponse à un message d'enregistrement local (*Local Registration*). Et enfin, il peut également mettre à jour une correspondance entre FEC et adresse IP en réponse à un message de redirection (*Redirect message*).

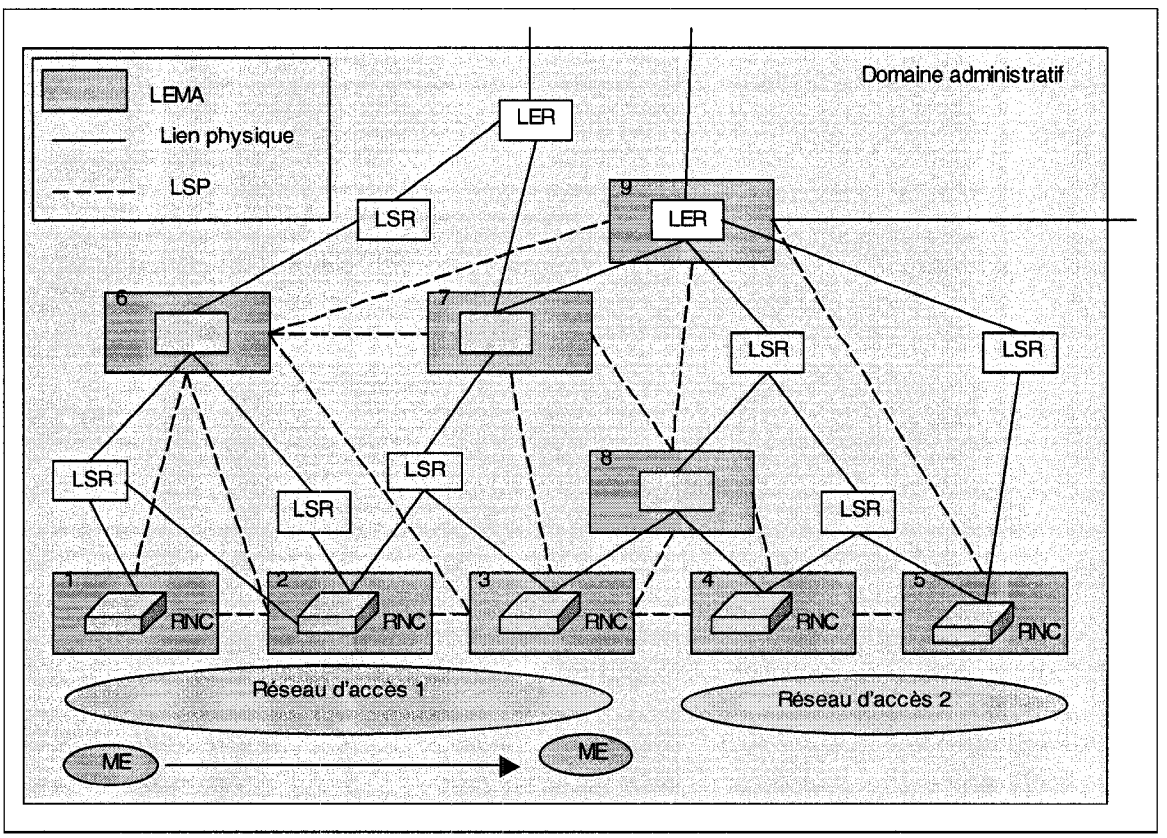
Essentiellement, le LEMA maintient la correspondance entre adresse IP et FEC en réponse aux mécanismes réguliers du plan de contrôle du routage et également des messages de signalisation contrôlés par la mobilité. Ainsi, lorsqu'un usager mobile entre dans la région de couverture d'un RNC, géré par le même LEMA que son précédent RNC, un message de signalisation est envoyé au LEMA afin qu'il modifie la FEC de l'adresse IP de l'usager mobile. Le LSP associé pointe alors vers le nouveau RNC. De même, si l'usager mobile change de LEMA, la FEC est modifiée en conséquence pour refléter ce changement.

Cette micro mobilité basée MPLS permet de gérer la mobilité en changeant dynamiquement la correspondance entre adresse IP et FEC grâce à des messages de signalisation, sans surcharger le plan de données et sans modifier la pile de protocoles.

Un domaine MPLS peut intégrer le schéma de micro mobilité basée MPLS en ajoutant la fonctionnalité de LEMA à un sous-ensemble de nœuds LSR. Comme on peut le voir à la Figure 2.6, les nœuds LEMA ne se situent pas obligatoirement en bordure d'un segment MPLS comme les LERs. Ils forment un réseau dont les nœuds sont reliés par des LSPs préétablis. Puisqu'ils permettent un changement de correspondance entre FEC et adresse IP contrôlée par la mobilité, les nœuds LEMA fournissent également les services d'un HA local à l'usager mobile. Tout usager dont l'adresse IP ne correspond pas à l'adresse du sous-réseau supporté par le RNC peut utiliser ce service en plus de la mobilité à grande échelle. Pour faciliter la mise en œuvre de ce service, le RNC doit annoncer la liste des LEMAs accessibles ainsi que

la manière dont ils sont disposés. L'usager choisit alors de s'enregistrer auprès d'un ou plusieurs agents et construit, sans aucune contrainte, sa propre chaîne hiérarchique de HA locaux. S'enregistrer à un certain niveau entraîne la mise en correspondance entre l'adresse IP de l'usager et un LSP qui pointe vers l'agent du niveau inférieur. Pour un usager donné, l'agent du niveau le plus bas fait la correspondance avec la station de base tandis que l'agent du niveau le plus élevé fournit la COA pour la mobilité à grande échelle.

Figure 2.6 Un réseau de LEMA



Par exemple, en se référant à la Figure 2.6, lorsque l'usager mobile se déplace du RNC_1 au RNC_3, il s'enregistre d'abord auprès du $LEMA_1$. Quand l'usager mobile est à la portée du RNC_2, il s'enregistre avec la chaîne (2,6,9). Le mouvement du

RNC_2 au RNC_3 entraîne un unique changement dans la chaîne qui devient (3,6,9). Tout changement du LEMA de niveau le plus élevé, dans notre cas du $LEMA_1$ au $LEMA_9$, résulte en un réenregistrement auprès du HA de l'usager mobile.

Il faut également noter que puisque l'adresse IP de l'usager mobile ne peut être utilisée pour le routage dans le domaine de micro mobilité, tous les LEMAs auprès desquels l'usager mobile est enregistré doivent avoir une entrée pour ce dernier dans leur table d'expédition afin de faire la correspondance entre l'adresse de l'hôte et l'étiquette MPLS appropriée.

Dans cette section, nous avons examiné deux mécanismes de support de la mobilité dans MPLS : MPLS mobile et la micro mobilité basée MPLS. Le premier mécanisme réalise l'intégration de la mobilité IP avec le protocole MPLS et gère donc une mobilité à grande échelle. Le second mécanisme, en revanche, gère une mobilité plus restreinte et a donc moins d'intérêt pour nous.

Ce chapitre nous a permis d'approfondir notre connaissance des différents concepts impliqués dans ce travail. Ainsi nous avons pu déterminer les origines de la dépendance géographique de l'APN dans les réseaux UMTS. Le protocole MPLS a également été brièvement décrit afin de pouvoir aborder l'étude des VPNs basés MPLS. L'accent a été mis sur les VPN BGP/MPLS qui permettent la commutation du trafic de données basée sur la correspondance entre les adresses VPN-IP et les étiquettes MPLS. Nous avons poursuivi en identifiant différents mécanismes pour supporter le protocole IPv6 et la mobilité dans MPLS.

CHAPITRE 3
MÉCANISMES D'ABOLITION D'ANCRAGE GÉOGRAPHIQUE DANS LES RÉSEAUX UMTS

Avec les années, la mobilité s'est profondément ancrée dans le comportement des populations des pays développés. Les gens se déplacent plus et de plus en plus loin que ce soit pour des motifs personnels ou professionnels. Le problème de l'ancrage géographique causé par l'APN dans un contexte de réseau visité, même s'il est toléré aujourd'hui, deviendra très vite problématique à mesure que le nombre de clients en déplacement augmentera. Dans ce chapitre, nous commençons par rappeler brièvement les faiblesses du mécanisme existant, puis nous dressons la liste des requis de la solution attendue avant de décrire le mécanisme que nous proposons.

3.1 Motivations et fondements

Le présent mémoire traite de la gestion de mobilité dans les réseaux UMTS et plus particulièrement de la gestion de la mobilité des usagers entre deux réseaux UMTS différents. Comme nous l'avons décrit dans le chapitre précédent, l'APN (*Access Point Name*) a un rôle important dans les mécanismes existants pour administrer ce type de mobilité. En effet, ce nom conforme au DNS (*Domain Name System*) fait référence au GGSN auprès duquel l'usager mobile s'enregistre. Il permet à ce dernier d'envoyer et de recevoir des paquets. Lors de la procédure d'activation d'un *PDP context*, le SGSN servant l'usager mobile met en œuvre un mécanisme de sélection qui aboutit à l'élection d'un APN. Ce dernier peut appartenir à un GGSN

du réseau visité ou à un GGSN du réseau d'origine de l'usager. Et c'est cette dernière option qui s'impose le plus souvent.

Ainsi, dans la majorité des cas, les paquets d'un usager mobile (MUA) originaire d'un réseau UMTS A et en visite dans un réseau B, devront d'abord transiter par un GGSN situé dans le réseau A avant de parcourir un autre segment de réseau pour rejoindre leur destinataire CN. Quand les réseaux A et B sont relativement proches géographiquement, les délais occasionnés peuvent être encore tolérés. Mais à mesure que la distance entre les deux réseaux augmentent et atteint une dimension intercontinentale, les problèmes engendrés par ces délais prennent un peu plus d'ampleur. Sans oublier que dans le scénario décrit ci-dessus, seul l'usager mobile MUA est en visite dans un autre réseau que le sien. Or, il se peut que le CN soit également en visite dans un réseau étranger et dans un tel cas, les données devront parcourir deux segments de réseaux supplémentaires avant d'atteindre leur destination. Ces délais sont inacceptables dans la mesure où la qualité de service tend à devenir une caractéristique cruciale dans les réseaux de prochaines générations.

De plus, il faut souligner l'utilisation des ressources sur les différents segments de réseaux empruntés par les données. En effet, ce sont autant de routeurs, de passerelles, de satellites et de liens qui verront leur charge augmenter avec le taux croissant de mobilité des usagers. Avec un tel mécanisme, un nombre grandissant d'usagers en déplacement pourrait conduire à une surcharge, voire une saturation des ressources. Une solution serait de limiter le nombre d'usagers pouvant bénéficier de services lors de leurs changements de réseau mais cela pourrait conduire à des pertes de revenus ou de la clientèle. En résumé, le mécanisme actuel de gestion de la mobilité des usagers entre différents réseaux UMTS, introduit un certain gaspillage de ressources des réseaux qu'il est impératif de résoudre.

3.2 Le mécanisme d'abolition de l'ancrage géographique

Le mécanisme d'abolition de l'ancrage géographique dans les réseaux UMTS est constitué d'un ensemble de nouvelles procédures ainsi que de modifications de certaines procédures existantes. Cette section et les suivantes sont consacrées à les décrire.

3.2.1 Présentation générale

Deux idées maîtresses ont présidé à la mise au point de ce mécanisme :

- S'inspirer autant que possible de Mobile IP version 6 qui est le protocole de référence pour la gestion de la mobilité à grande échelle dans le monde IP ;
- Modifier les différentes procédures afin que l'usager mobile choisisse le service qu'il désire et non le GGSN capable de le lui rendre lors de l'activation du *PDP Context.*

La mise en œuvre d'un tel mécanisme requiert tout d'abord l'existence d'un système d'identification ou de classement des services uniforme et homogène entre les PLMN partenaires. Un tel système, que nous avons baptisé *ServiceID*, devrait permettre à l'usager mobile de désigner sans ambiguïté le service qu'il demande. Une fois, le service désiré identifié, le SGSN doit déterminer dans quel PLMN se situera le GGSN qui le fournira. L'une des étapes du mécanisme de sélection de l'APN remplissait ce rôle jusqu'à présent. Mais, avec le remplacement de l'APN par le *ServiceID* et la modification du principe même de sélection, nous avons dû apporter des changements au mécanisme et le rebaptiser : mécanisme de sélection du GGSN. Après son exécution, le SGSN possède le *ServiceID* du service désiré par le MN ainsi que le PLMN dans lequel doit se trouver le GGSN fournissant ce service. Il doit à présent trouver l'adresse IP de ce GGSN.

Actuellement, la recherche de cette adresse est effectuée à l'aide d'une requête DNS envoyée par le SGSN à un serveur DNS. L'APN, qui est un nom conforme au

DNS, sert de référence au GGSN choisi. Dans notre nouveau mécanisme d'abolition d'ancrage géographique, l'APN est remplacé par le *ServiceID*. Une requête DNS n'est donc plus possible. Nous avons alors mis au point deux procédures afin de remplacer la base de données que représente le serveur DNS. La première a pour but de peupler la base de données qui n'est plus centralisée dans un serveur mais «clonée» sur chaque SGSN du PLMN. La procédure de construction de la liste des GGSN permet à ces derniers d'informer les SGSN des services qu'ils fournissent. La seconde, en revanche, permet à un SGSN d'interroger la base de données d'un pair dans un autre PLMN. La procédure de découverte de l'adresse d'un HGGSN, comme son nom l'indique, fournit l'adresse IP d'un GGSN situé dans le réseau d'origine de l'usager mobile et répondant à certaines caractéristiques.

Tous les changements cités précédemment affectent directement les procédures reliées au *PDP Context* et principalement celle de l'activation. Dans les sections suivantes, nous tâcherons de décrire ces modifications.

3.2.2 Système de *ServiceID*

L'idée est de développer un système qui sera apte à remplacer l'actuel *Access Point Name*. Ce système sera utilisé par les nœuds GSN de PLMN différents qui n'auront pas obligatoirement conclu des accords concernant le *roaming* de leurs usagers respectifs.

Afin de préciser les caractéristiques attendues du système à élaborer, rappelons les attributs et fonctions de l'APN. L'*Access Point Name* remplit 2 fonctions principales :

- il permet de désigner sans ambigüité le *Packet Data Network* auquel l'usager mobile désire accéder ;
- il peut identifier un service que l'usager désire utiliser.

L'APN est donc un nom *Domain Name System* (DNS) qui fait référence au GGSN qui donne accès à un PDN particulier ou à un service bien précis. Une simple requête à un serveur DNS fournit l'adresse IP du GGSN désigné par l'APN. Par ailleurs, l'APN possède également les caractéristiques reliées suivantes:

- Une paire (APN, *PDP Address*) identifie un groupe de *PDP Contexts* possédant des caractéristiques de qualité de service différentes qui doivent être traitées de la même façon ;
- L'utilisation d'une autoconfiguration d'adresse *stateless* ou *stateful* est configurée par APN ;
- Chaque *PDP Type* possède un APN par défaut ;
- Un usager peut avoir plusieurs enregistrements pour le même *PDP Type* et la même *PDP Address* mais avec des APN différents ;
- Un usager peut avoir jusqu'à deux enregistrements pour le même *PDP Type* et le même APN: un pour une *PDP address* statique et un autre pour une *PDP address* dynamique ;
- L'APN *wild card* signifie qu'un APN par défaut doit être choisi par le SGSN si aucun APN n'est requis par l'usager et qu'un *PDP Context* avec un *PDP Address* dynamique peut être activé avec n'importe quel APN demandé par l'usager.

Le système que nous avons baptisé *ServiceID* devra donc remplir les mêmes fonctions de désignation de PDN et d'identification de services de l'APN et satisfaire à ses caractéristiques secondaires. Cependant le système *ServiceID* se distingue de l'APN sur les points suivants:

- Le *ServiceID* est un nombre et non un nom conforme au DNS ;
- Contrairement à l'APN qui fait référence de façon spécifique à un GGSN dans un PLMN donné et qui posséde donc un certain ancrage géographique, le *ServiceID* fait référence à un PDN ou à un service. En fonction du PLMN

dans lequel se trouve l'usager mobile, un GGSN capable de fournir l'accès au PDN ou au service désiré sera choisi par le SGSN.

L'ancrage géographique de l'APN est donc éliminé dans le système *ServiceID* puisque le choix du GGSN est fait en fonction de la localisation de l'usager mobile à condition que le PLMN dans lequel se trouve ce dernier ait des accords de *roaming* aver le PLMN d'origine. Dans le cas contraire, le GGSN choisi appartient au PLMN d'origine de l'usager. La correspondance entre le *ServiceID* et l'adresse IP du GGSN adéquat n'est pas obtenue par une requête DNS comme pour l'APN mais grâce à une recherche exhaustive dans une liste (*ServiceID*, Adresse IP de GGSN) détenue par chaque SGSN d'un PLMN. Les mécanismes de construction et de mise à jour de cette liste seront abordés dans les sections suivantes.

Le *ServiceID* doit remplir deux fonctions principales. Aussi la définition de ce système comporte-t-elle deux grandes parties, chacune adressant une fonction particulière. Commençons par la fonction la plus sollicitée : la désignation d'un PDN. Un PDN est un réseau fournissant un service de données. Un exemple de ce type de réseau est l'Internet. Chaque PLMN peut être connecté à plusieurs PDNs par l'intermédiaire d'un ou plusieurs GGSNs. Avec l'APN, on peut décrire le point d'accès à un PDN dans un PLMN bien particulier. Le *ServiceID*, en revanche, doit décrire le point d'accès à un PDN indépendamment du PLMN. Il faut donc que l'identifiant représenté par le *ServiceID* puisse être reconnu dans tous les PLMN comme faisant référence à un PDN donné. L'identifiant en question est le *Autonomous System Number.*

L'*Autonomous System Number* (ASN) est un nombre permettant d'identifier de façon unique chaque *Autonomous System* (AS). Un AS est un groupe de réseaux IP administrés par un ou plusieurs opérateurs partageant une seule politique de routage. Les ASN sont assignés par la *Internet Assigned Number Authority* (IANA) qui alloue des blocs de numéros aux *Regional Internet Registries* (RIR). Le RIR local assigne alors un ASN à une entité à partir du bloc qu'il a reçu. Les ASN sont généralement des

entiers de 16 bits qui permettent au maximum 65536 assignations. Ils sont divisés en 2 intervalles. Le premier [1,64511] est réservé aux ASN publics qui peuvent être utilisés sur l'Internet. Le second intervalle [64512,65536] est réservé aux ASN privés qui sont uniquement à usage interne d'une organisation. Actuellement, l'IETF possède plusieurs *drafts* qui définissent des mécanismes décrivant l'utilisation de ASN de 32 bits. En effet, à plus ou moins long terme, l'espace d'adressage des 16 bits risque de se révéler insuffisant. Les ASN de 16 bits existants ne seront pas remplacés. Aussi, nous utiliserons des ASN de 32 bits plutôt que de 16 bits par souci d'anticipation.

Les AS peuvent être regroupés en trois catégories en fonction de leurs connexions et de leur opération : les AS *multihomed*, les AS *stub*, les AS de transit. Les AS *multihomed* maintiennent des connexions avec plus d'un fournisseur de service. Cela leur permet de rester connecté à l'Internet dans l'éventualité où l'un des fournisseurs de service serait complètement en panne. De plus, ce genre de AS ne permettent pas au trafic d'un fournisseur de service de passer par le réseau d'un autre fournisseur. Les AS *stub*, en revanche, ne sont connectés qu'à un seul fournisseur de service et les AS de transit, quant à eux, permettent d'interconnecter différents réseaux.

L'ASN se révèle donc être un identifiant tout indiqué pour discriminer chaque réseau de données de façon unique mais également de façon indépendante des PLMN. De cette façon, l'identification des PDN n'aura pas à faire l'objet d'accords particuliers entre chaque paire de PLMN.

Intéressons-nous à présent à la seconde fonction principale de l'APN : il s'agit de l'identification d'un service. Notre objectif est de trouver une manière homogène de désigner des services dans les réseaux UMTS. Aussi, notre choix se porte naturellement sur l'architecture de qualité de service UMTS qui est partagée par les réseaux d'origine et visité. Cette architecture possède quatre classes de services ou de trafic :

- la classe conversational ;
- la classe streaming ;
- la classe interactive ;
- la classe background.

Le principal facteur distinctif entre ces classes de QoS est le degré de sensibilité au délai du trafic : la classe *conversational* correspond aux trafics très sensibles au délai tandis que la classe *background* correspond aux trafics les plus insensibles au délai.

La classe *conversational* a été conçue pour les conversations temps réel et est caractérisée par la préservation de la relation de temps entre les entités d'information du *stream* et par un délai de transfert très bas et rigoureusement soumis à la perception humaine de la conversation. Cette classe est indiquée pour la téléphonie, la voix sur IP ou la vidéo conférence.

Pour la classe *streaming*, en revanche, même s'il n'y a aucune restriction sur le délai de transfert, celui-ci doit avoir une variation assez limitée pour préserver la relation de temps entre les entités d'information du *stream*. Cette classe s'adresse donc au jeu de contenu audio ou vidéo, donc aux *streams* temps réel.

La classe *interactive*, comme son nom l'indique, a été conçue pour le trafic interactif. Ainsi, ses caractéristiques fondamentales sont le modèle requête-réponse et la préservation de la charge utile. Il s'agit de la classe du *web browsing*, de l'accès à un serveur ou de l'interrogation automatique de bases de données.

La classe *background* pour le trafic d'arrière plan est caractérisée par le fait que le destinataire n'attend pas les données avant un certain temps et que le contenu de la charge utile doit être préservé.

Ces classes permettront à l'usager de désigner le service qu'il désire par le biais des caractéristiques de qualité de service que ce dernier exige.

Nous avons défini les bases du système de *ServiceID* et nous avons à présent à en définir la forme. Contrairement à l'APN qui est un nom conforme au DNS de

100 octets au maximum, le *ServiceID* est un nombre représenté avec exactement 5 octets. Le format de ce dernier est illustré au Tableau 3.1.

Tableau 3.1 Format du *ServiceID*

0 0 0 0 0 0 0 0 0 1 2 3 4 5 6 7	0 0 1 1 1 1 1 1 8 9 0 1 2 3 4 5	1 1 1 1 2 2 2 2 6 7 8 9 0 1 2 3	2 2 2 2 2 2 3 3 4 5 6 7 8 9 0 1	3 3 3 3 3 3 3 3 2 3 4 5 6 7 8 9
Fonction	ASN ou classe de service			

Le premier octet constitue le champ Fonction. Il sert à discriminer la fonction remplie par le *ServiceID* : l'identification d'un PDN ou d'un service. Le champ Fonction peut prendre les valeurs suivantes :

- 0 (0b00000000) : cette valeur correspond au *ServiceID wild card* ;
- 1 (0b000000001) : cette valeur indique que le *ServiceID* désigne un PDN ;
- 3 (0b000000011) : cette valeur indique que le *ServiceID* désigne un service.

À ce jour, ce sont les seules valeurs que peut prendre le champ Fonction. Si ce champ contient d'autres valeurs que celles définies, le *ServiceID* sera considéré comme invalide ou erroné.

En fonction de la valeur du champ Fonction, les quatre derniers octets du *ServiceID* auront différentes valeurs et significations. Lorsque le champ Fonction possède la valeur 0, le nombre représenté par les 4 derniers octets sera 0. Ainsi, le *ServiceID wild card* aura globalement une valeur de 0. En revanche, pour un champ Fonction contenant la valeur 1, les quatre derniers octets représenteront un *Autonomous System Number* de 32 bits désignant un PDN donné. Enfin, pour un champ Fonction avec la valeur 3, les quatre derniers octets pourront prendre exactement 4 valeurs correspondant aux quatre classes de service UMTS :

- 1.0.0.0 (0b00000001.00000000.00000000.00000000) : cette valeur correspond à la classe *conversational* ;
- 3.0.0.0 (0b00000011.00000000.00000000.00000000) : cette valeur correspond à la classe *streaming* ;

- 7.0.0.0 (0b00000111.00000000.00000000.00000000) : cette valeur correspond à la classe *interactive* ;
- 15.0.0.0 (0b00001111.00000000.00000000.00000000) : cette valeur correspond à la classe *background.*

Le *ServiceID* remplit donc les deux fonctions principales de l'APN. Les sections suivantes permettront de préciser comment le *ServiceID* assure l'identification d'un GGSN. Qu'en est-il des propriétés secondaires que possèdent l'APN ?

- Une paire (*ServiceID*, *PDP Address*) peut identifier un groupe de *PDP Contexts* possédant des caractéristiques de qualité de service différentes puisque dans l'architecture UMTS, le profil de QoS dépend d'attributs qui peuvent prendre différentes valeurs pour une même classe de service.
- L'utilisation d'une autoconfiguration d'adresse *stateless* ou *stateful* peut être configurée par *ServiceID* ;
- Chaque *PDP Type* peut possèder un *ServiceID* par défaut ;
- Un usager peut avoir plusieurs enregistrements pour le même *PDP Type* et la même *PDP Address* mais avec des *ServiceID* différents ;
- Un usager peut avoir jusqu'à deux enregistrements pour le même *PDP Type* et le même *ServiceID*: un pour une *PDP address* statique et un autre pour une *PDP address* dynamique ;
- Le *ServiceID wild card* remplit les mêmes fonctions que l'APN *wild card.*

Le *ServiceID* est donc apte à remplacer l'actuel APN. Il possède les mêmes fonctions et les mêmes propriétés mais il n'est pas handicapé par un ancrage géographique. Par ailleurs, le *ServiceID* n'est représenté que par 5 octets contre les 100 octets maximum de l'APN. Cela représente un gain non négligeable en mémoire lorsque l'on sait qu'un usager peut possèder plusieurs PDP *Contexts* par *ServiceID* et que les nœuds GSN s'occupent de milliers d'usagers.

Nous avons défini le modèle de remplacement de l'APN. Les sections suivantes décriront les modifications à apporter pour intégrer ce modèle de *ServiceID* à la procédure d'activation de PDP *Context.*

3.2.3 Procédure de construction de la liste des GGSN

Cette procédure fait partie de la paire de procédures mises au point pour remplacer l'utilisation du serveur DNS pour la découverte des adresses IP de GGSN. Elle a pour protagonistes les nœuds GSN et pour médium un message *Router Advertisement* modifié. Il s'agit en quelque sorte d'une procédure de peuplement de base de données, qui prend ici la forme de listes *ServiceID*-Adresse IP indexées par *ServiceID.* Ces listes sont situées dans les nœuds SGSN qui les construisent à partir des informations contenues dans les messages *Router Advertisement* envoyés par les GGSN.

La procédure de construction de la liste de GGSN s'inspire d'une procédure similaire du protocole Mobile IP version 6. En effet, MIPv6 utilise une procédure modifiée de *Neighbor Discovery* pour la construction d'une liste des routeurs fonctionnant comme HA sur le lien. Le format du message *Router Advertisement* a été modifié en y ajoutant un nouveau drapeau d'un bit (H) pour indiquer que le routeur émetteur du message sert comme HA sur le lien en question. De nouvelles options ont également été définies

De la même manière, nous avons donc modifié le format du message *Router Advertisement* de MIPv6 en y ajoutant un nouveau drapeau (G) pour indiquer que le routeur émetteur du message en question sert comme GGSN. De plus, nous avons créé une nouvelle option : GGSN *Information* afin de transmettre toutes les informations pertinentes sur les GGSN. Le format du message *Router Advertisement* modifié est présenté au Tableau 3.2 immédiatement suivi de la description des champs.

Tableau 3.2 Format du message *Router Advertisement* modifié

Type	Code				Checksum
Cur Hop Limit	M	O	H	Reserved	Router Lifetime
Reachable time					
Retrans timer					
Options					

- Type = 134 ;
- Code = 0 ;
- Checksum : «somme de vérification» ICMP ;
- Cur Hop Limit : entier non signé de 8 bits, indiquant la valeur par défaut placée dans le champ *Hop Count* de l'en-tête IP des paquets IP sortants ;
- Managed Address Configuration (M) : lorsque ce bit est actif, les hôtes utilisent le protocole *stateful* pour l'auto configuration des adresses ayant déjà utilisées l'auto configuration *stateless* ;
- Other stateful configuration (O) : lorsque ce bit est actif, les hôtes utilisent le protocole *stateful* pour l'auto configuration des autres informations (pas des adresses) ;
- Home Agent (H) : ce bit est activé pour indiquer que le routeur qui a envoyé ce *Router Advertisement* fonctionne également comme HA sur ce lien ;
- GGSN (G) : ce bit est mis pour indiquer que le routeur qui a envoyé ce RA fonctionne également comme GSSN ;
- Reserved : champ de 4 bits inutilisé ;
- Router Lifetime : entier non signé de 16 bits indiquant la durée de vie associée au routeur par défaut en secondes (max : 18.2h) ;

- Reachable time : entier non signé de 32 bits indiquant le temps en millisecondes durant lequel le nœud suppose que son voisin est joignable après avoir reçu un message de *reachability confirmation* ;
- Retrans timer : entier non signé de 32 bits indiquant le temps en millisecondes entre deux messages *Neighbor Sollicited* retransmis ;
- Options : aux options déjà définies par les protocoles *Neighbor Discovery* [8], RFC 3775 [7], nous ajoutons l'option *GGSN Information.*

Nous poursuivons en décrivant la nouvelle option *GGSN Information* utilisée dans les *Router Advertisements* envoyés par un GGSN pour publier les informations spécifiques à cette fonctionnalité de routeur. Le format de l'option est présenté au Tableau 3.3 :

Tableau 3.3 Format de l'option GGSN Information

Type	Length	Reserved
GGSN Preference		GGSN Lifetime
ServiceIDs		

- Type : option de *Neighbor Discovery* ;
- Length : entier non signé de 8 bits indiquant la longueur de l'option ;
- Reserved : ce champ est inutilisé. Il doit être initialisé à 0 par l'envoyeur et ignoré par le destinataire ;
- GGSN Preference : entier non signé de 16 bits indiquant les préférences du GGSN. Une valeur élevée indique une haute disponibilité. Il est utilisé pour ordonner la liste des GGSN. Si cette option n'est pas incluse dans un RA dans lequel le bit G est mis, cela signifie que la valeur du champ GGSN Preference est 0.

- Le GGSN auteur du RA devrait déterminer dynamiquement la valeur du champ *GGSN Preference*, en se basant par exemple, sur le nombre de MN qu'il sert présentement ou sur les ressources encore disponibles pour servir d'autres MN. Le mécanisme utilisé par le GGSN pour déterminer la valeur du champ dépasse le cadre de ce mémoire mais il doit être approprié ;
- GGSN Lifetime : entier non signé de 16 bits indiquant la durée de vie du GGSN en secondes. Par défaut, ce champ prend la valeur de la durée de vie du routeur telle que spécifiée dans le corps principal du *Router Advertisement.* Une valeur de 0 ne doit pas être utilisée. GGSN Lifetime s'applique uniquement à l'utilité du routeur en tant que GGSN et non aux informations contenant dans les autres champs ou options du message ;
- *ServiceIDs* : liste des *ServiceIDs* des services que le GGSN est en messure de fournir. Les *ServiceIDs* sont placés les uns à la suite des autres. Leur taille fixe de 5 octets permet de les récupérer par simple *parsing.*

Les routeurs GGSN ne possèdent pas de liste des autres GGSN servant sur le PLMN. Ce sont eux qui expédient les RA multicast à intervalle de temps aléatoire tel que décrit dans le protocole *Neighbor Discovery* [8]. Ils possèdent tous une *Advertising Interface.* Ces RA respectent le format des RA modifié présenté précédemment. Les GGSN ne reçoivent pas de RA des autres GGSN, ni des SGSN. L'échange de messages se fait à sens unique des GGSN vers les SGSN.

Pour le domaine qu'il couvre, le routeur servant comme SGSN doit maintenir une liste des GGSN contenant toutes les informations à propos des VGGSN dans ce domaine. Cette liste est par la suite utilisée par le SGSN lors de la procédure d'activation de *PDP context* d'un MN pour la sélection du GGSN qui servira le MN. Les informations de cette liste sont reçues des messages périodiques non sollicités *Router Advertisements* multicast. Ces *Router Advertisements* proviennent des GGSN dans le domaine et ont le drapeau GGSN (G) mis.

Sur réception d'un *Router Advertisement* valide telle que définit par l'algorithme de traitement spécifié par le protocole *Neighbor Discovery* [8], le SGSN accomplit les étapes suivantes en plus de celles déjà requises par le protocole *Neighbor Discovery* et par MIPv6 [7] :

- Si le bit GGSN (G) n'est pas mis dans le message *Router Advertisement*, effacer l'entrée du nœud expéditeur de la liste des VGGSN (si elle existe). Sauter les étapes suivantes ;
- Sinon, extraire l'adresse source de l'en-tête IP du *Router Advertisement*. Il s'agit de l'adresse du GGSN expéditeur du message ;
- Déterminer la préférence pour ce VGGSN. Si le *Router Advertisement* contient une option *GGSN Information*, alors la valeur de la préférence est prise du champ GGSN Preference de l'option ; sinon, la préférence par défaut de 0 doit être utilisée ;
- Déterminer la durée de vie pour ce GGSN. Si le *Router Advertisement* contient une option *GGSN Information*, alors la valeur de la durée de vie est prise du champ GGSN Lifetime de l'option ; sinon, la durée de vie spécifiée dans le champ Router Lifetime dans le *Router Advertisement* doit être utilisée ;
- Si l'adresse IP du VGGSN expéditeur du RA est déjà présente dans la liste de GGSN du SGSN et que la valeur de la durée de vie reçue est 0, effacer immédiatement cette entrée de la liste ;
- Sinon, si l'adresse IP du GGSN expéditeur du RA est déjà présente dans la liste de GGSN du SGSN, mettre à jour les valeurs de la durée de vie et de la préférence avec les valeurs déterminées précédemment ;
- Si l'adresse IP du GGSN expéditeur du RA est absente de la liste de GGSN du SGSN et que la valeur de la durée de vie reçue n'est pas nulle, créer une nouvelle entrée dans la liste et initialiser sa durée de vie et sa préférence aux valeurs déterminées précédemment ;
- Si l'entrée de la liste de GGSN pour l'adresse IP du GGSN n'a pas été effacée comme décrit précédemment, initialiser ou mettre à jour la liste des PDN et services accessibles par ce GGSN à partir de l'option GGSN Information.

Figure 3.1 Algorithme de traitement d'un *Router Advertisement* modifié

Les routeurs SGSN n'expédient aucun message aux GGSN dans le cadre de cette procédure de construction de liste des VGGSN.

3.2.4 Procédure de découverte de l'adresse d'un HGGSN

Cette procédure a pour but d'obtenir l'adresse IP d'un GGSN se trouvant dans le PLMN d'origine du mobile et donnant accès au service ou au PDN demandé par ce dernier.

Dans un PLMN, la procédure de construction de la liste des GGSN permet à chaque SGSN de connaître les différents services fournis par les GGSN du domaine. Cette liste sert pour l'obtention de l'adresse IP d'un GGSN pour un MN à domicile ou en provenance d'un autre PLMN. Pour un SGSN, la liste de GGSN en opération dans un autre PLMN est inaccessible. Il s'agit donc de mettre en place une procédure permettant à un SGSN d'obtenir l'adresse IP d'un GGSN fournissant un service particulier dans un autre PLMN.

Cette procédure s'effectue sous la forme d'un échange de messages entre le SGSN du PLMN visité (VSGSN) et un SGSN du PLMN d'origine du MN (HSGSN). Le message envoyé par le VSGSN contient le *ServiceID* du service que doit fournir le GGSN. Il est adressé à une adresse permettant de rejoindre tous les SGSN du HPLMN. Sa forme est voisine de celle d'un message *Router Sollicitation* du protocole *Neighbor Discovery* avec en plus le *ServiceID*. Nous baptisons ce message : *ICMP Home GGSN Address Discovrey Request.*

Le SGSN qui reçoit ce message *ICMP Home GGSN Address Discovrey Request* effectue une recherche dans sa liste de GGSN avec comme clé le *ServiceID* contenu dans le message. Peu importe le résultat de la recherche, le SGSN répond avec un message *ICMP Home GGSN Address Discovrey Response.* Ce dernier contient un code de succès ainsi que l'adresse du GGSN trouvée en cas de succès de la recherche. En

revanche, le message ne contient que le code d'échec et la cause de celui-ci en cas d'échec de la recherche.

Contrairement à la procédure de construction de la liste des GGSN qui est périodique et non sollicitée, cette procédure-ci n'intervient que lorsque durant le mécanisme de sélection du GGSN, un accès par le HPLMN est sélectionné.

Le message *ICMP Home GGSN Address Discovery Request* est envoyé par le SGSN du réseau visité à un SGSN du réseau domicile du MN en *roaming* dans le cadre de la procédure de découverte de l'adresse IP d'un HGGSN. Ce message est envoyé à l'adresse *unicast* des GGSN du réseau domicile du MN en roaming. Son format est présenté au Tableau 3.4.

Tableau 3.4 Format du message *ICMP Home GGSN Address Discovery Request*

Type	Code	Checksum
Identifier		Reserved
Service ID		

- Type : 154 (à définir de façon cohérente avec les valeurs des autres messages ICMP) ;
- Code : 0 ;
- Checksum : «somme de vérification» ICMP ;
- Identifier : identifiant permettant d'apparier un message *ICMP Home GGSN Address Discovery Request* avec le message *ICMP Home GGSN Address Discovery Response* correspondant ;
- Reserved : réservé pour usage futur. Initialiser à 0 ;
- *ServiceID* : *ServiceID* du service que doit fournir le GGSN désiré.

Le message *ICMP Home GGSN Address Discovery Response* est utilisé par le SGSN du réseau domicile du MN en *roaming* pour répondre au SGSN du réseau visité qui a initié la procédure de découverte de l'adresse IP du HGGSN. Son format est présenté au Tableau 3.5.

Tableau 3.5 Format du message *ICMP Home GGSN Address Discovery Response*

Type	Code	Checksum
Identifier		Reserved
Home GGSN Address		

- Type : 155 (à définir de façon cohérente avec les valeurs de ce champ pour les autres messages ICMP) ;
- Code : ce champ indique si la recherche dans la liste de GGSN a été fructueuse ou non. Une valeur entre 0 et 127 indique un succès. Dans ce cas, le champ Home GGSN Address contient effectivement l'adresse IP du GGSN désiré. En revanche, si la valeur du code est comprise entre 128 et 255, cela indique qu'il y a eu une erreur explicitée dans le champ Home GGSN Address ;
- Checksum : «somme de vérification» ICMP ;
- Identifier : identifiant provenant du message *ICMP Home GGSN Address Discovery Request* ;
- Reserved : réservé pour usage futur. Initialiser à 0 ;
- Home GGSN Address : selon la valeur du champ Code, ce champ contient l'adresse IP du GGSN trouvée lors de la recherche par *ServiceID* ou la cause de l'erreur survenue.

3.2.5 Mécanisme de sélection du GGSN

En analysant le mécanisme de sélection de l'APN, on constate immédiatement que les 3/4 des cas qui n'aboutissent pas directement à un rejet de la procédure d'activation de *PDP Context* correspondent à la sélection de l'APN d'un GGSN du HPLMN. Si on ne s'intéresse qu'aux cas dans lesquels le MN n'est pas dans son HPLMN, la proportion devient un pour deux. Et c'est cette proportion qu'il nous faut faire tendre vers 100%.

La procédure que nous voulons mettre au point a pour but de trouver le GGSN du PLMN dans lequel se trouve le MN capable de lui fournir l'accès au PDN ou au service qu'il désire. Le mécanisme courant de sélection de l'APN comporte essentiellement trois étapes :

- La première détermine le mode de sélection de l'APN à partir de la présence ou de l'absence de certains paramètres dans le message *Activate PDP Context Request* ou dans le(s) enregistrement(s) pour le MN dans le HLR ;
- La seconde consiste à déterminer à quel PLMN appartiendra le GGSN dont l'APN sera sélectionné ;
- La dernière correspond à l'interrogation du serveur DNS.

Notre mécanisme de sélection du GGSN comporte 3 étapes similaires :

- La première ne change pas à ceci près que l'APN est remplacé par le paramètre *ServiceID* : à la fin de cette étape, on obtient le *ServiceID* qui servira de clé pour la recherche dans la liste de GGSN ;
- La seconde (plus simple que celle du mécanisme de sélection de l'APN) permet de déterminer dans quel PLMN choisir le GGSN qui fournira le service identifié par le *ServiceID* ;
- La dernière consiste à effectuer la recherche dans la liste de GGSN indexée par *ServiceID*.

Détaillons à présent chacune des étapes du mécanisme de sélection du GGSN. La première étape détermine le mode de sélection du *ServiceID* parmi les suivants :

- ChoisiParMN ;
- ChoisiParSGSN ;
- Souscrit.

Si le mode sélectionné est ChoisiParMN, le *ServiceID* correspond à celui contenu dans le message *Activate PDP Context Request.* Si, en revanche, le mode choisi est Souscrit, le *ServiceID* est extrait du *PDP Context* identifié durant la détermination du mode de sélection. (Ce mode est implicitement associé avec des procédures d'activation de *PDP Context* secondaire). Enfin, le mode ChoisiParSGSN implique que le *ServiceID* par défaut associé au PDP type soit connu, sinon la demande d'activation de *PDP Context* est rejetée.

La seconde étape de détermination du PLMN et la troisième étape de recherche dans la liste de GGSN sont intimement liées. C'est pourquoi nous les explicitons dans l'algorithme décrit à la Figure 3.1.

L'algorithme est également illustré à la Figure 3.2.

L'étape 3 du mécanisme est constituée de la recherche dans la liste de GGSN et de la procédure de découverte de l'adresse du HGGSN. Cette dernière comporte également une recherche dans la liste de GGSN, telle que décrite précédemment. Le mode opératoire de cette recherche dépasse le cadre de ce mémoire. Cependant, il importe que la méthode utilisée se serve du *ServiceID* comme clé et qu'elle soit efficace et optimale.

1. Une fois en possession du *ServiceID*, le SGSN vérifie si le MN se trouve ou non dans son HPLMN "usager dans HPLMN ?" :
   - 1.1. "Oui, usager dans HPLMN", le SGSN effectue une recherche dans sa liste de GGSN indexée par *ServiceID* "Résultat de la recherche ?" :
     - 1.1.1. "Résultat de la recherche positif", la demande d'activation de *PDP Context* peut se poursuivre.
     - 1.1.2. "Résultat de la recherche négatif", la demande d'activation de *PDP Context* est rejetée.
   - 1.2. "Non, usager dans VPLMN", le SGSN s'assure que le MN peut utiliser les services d'un PLMN autre que le sien "Adresse VPLMN permise ? ":
     - 1.2.1. "Oui, adresse VPLMN permise", le SGSN vérifie que l'accès au point d'accès du VPLMN est autorisé, "VPLMN AP autorisé ? ":
       - 1.2.1.1. "Oui, VPLMN AP autorisé", le SGSN effectue une recherche dans sa liste de GGSN indexée par *ServiceID*, "Résultat de la recherche ? " :
         - 1.2.1.1.1. "Résultat de la recherche positif", la demande d'activation de *PDP Context* peut se poursuivre.
         - 1.2.1.1.2. "Résultat de la recherche négatif", le SGSN vérifie que l'accès au point d'accès du HPLMN est autorisé, "HPLMN AP autorisé ?" :
           - 1.2.1.1.2.1. "Oui, HPLMN AP autorisé", le SGSN lance la procédure de découverte de l'adresse IP d'un HGGSN avec le *ServiceID* obtenue précédemment, "Adresse IP du HGGSN obtenue ? " :
             - 1.2.1.1.2.1.1. "Oui, Adresse IP du HGGSN obtenue", la demande d'activation de *PDP Context* peut se poursuivre.
             - 1.2.1.1.2.1.2. "Non, Adresse IP du HGGSN introuvable", la demande d'activation de *PDP Context* est rejetée.
           - 1.2.1.1.2.2. "Non, HPLMN AP refusé", la demande d'activation de *PDP Context* est rejetée.
       - 1.2.1.2. "Non, VPLMN AP refusé", le SGSN vérifie que l'accès au point d'accès du HPLMN est autorisé, "HPLMN AP autorisé ? " → aller à 1.2.1.1.2.1. ou 1.2.1.1.2.2.
     - 1.2.2. "Non, adresse VPLMN interdite", le SGSN vérifie que l'accès au point d'accès du HPLMN est autorisé, "HPLMN AP autorisé ? " → aller à 1.2.1.1.2.1. ou 1.2.1.1.2.2.

Figure 3.2 Algorithme de sélection du GGSN

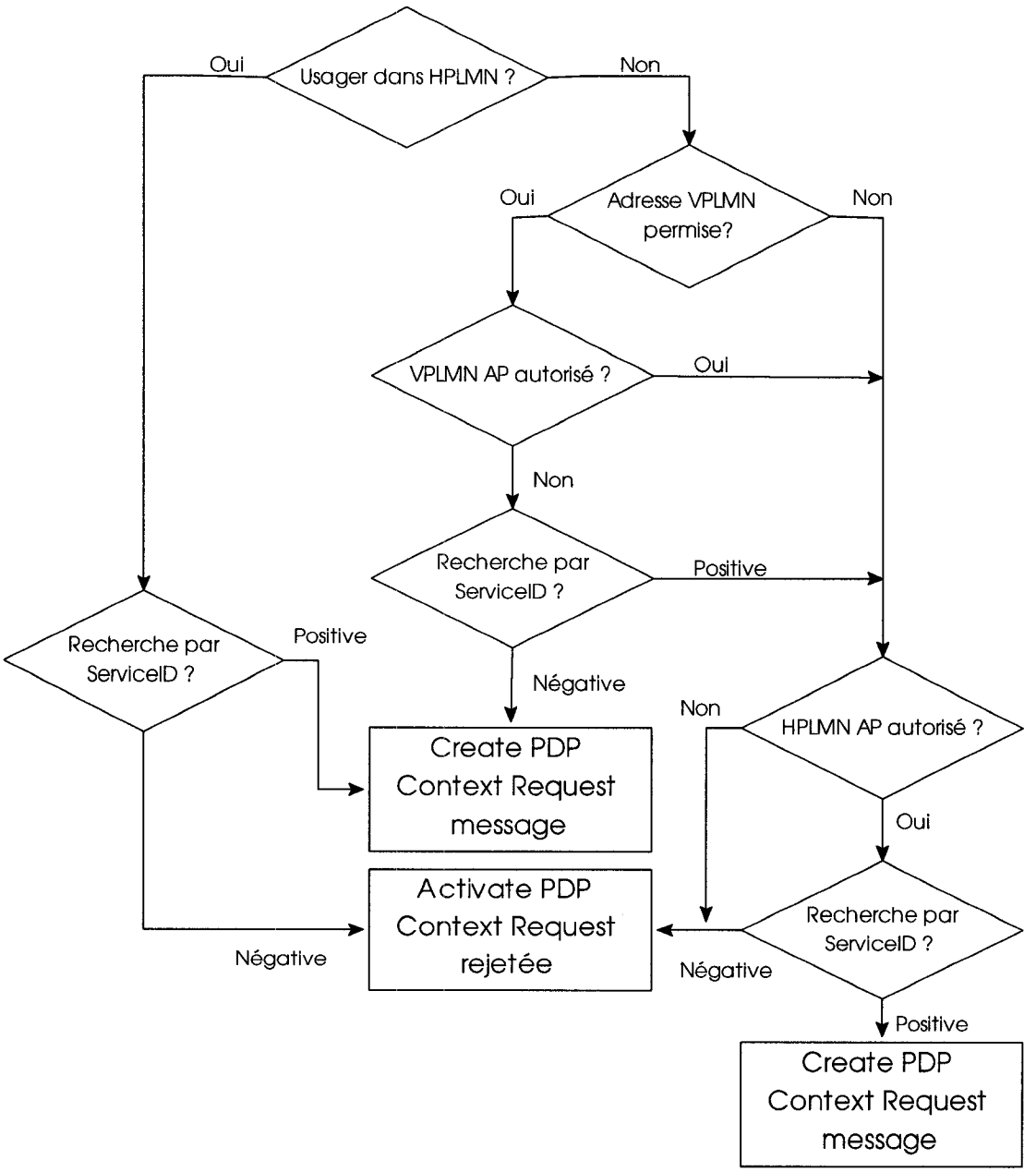


Figure 3.3 Seconde étape du mécanisme de sélection de l'APN

Il ne faut pas perdre de vue que nous voulons faire en sorte que la proportion des cas où un MN en *roaming* utilise un GGSN du réseau visité tende vers 100%. Pour que ce nouveau mécanisme de sélection atteigne cet objectif, on suppose que certaines hypothèses sont satisfaites :

- La majorité des usagers ont le droit d'utiliser les services d'un PLMN autre que le leur ;
- Les PLMNs permettant à leurs usagers d'utiliser leurs services respectifs doivent s'assurer qu'un ensemble de GGSN ou un GGSN fournit les services proposés par son pair.

3.2.6 Procédure d'activation de *PDP Context* modifiée

Les sections précédentes ont fourni une description détaillée des nouveautés et modifications apportées afin qu'un usager mobile en *roaming* n'ait plus à subir les délais liés à l'ancrage géographique de l'APN. À présent, il convient de décrire de quelle manière la procédure d'activation de *PDP Context* s'en trouve affectée.

Nous avons choisi de présenter des diagrammes de messages afin de mettre l'accent sur la chronologie de la procédure. Quatre scénarii pour lesquels les échanges de messages diffèrent ont été identifiés.

- Le premier scénario illustré par la Figure 3.3 correspond au cas où l'usager mobile se trouve dans son PLMN d'origine. En principe, ce cas de figure ne nous intéresse pas outre mesure mais puisque la procédure d'activation de *PDP Context* a été changée, il convient de décrire le déroulement de ce scénario :

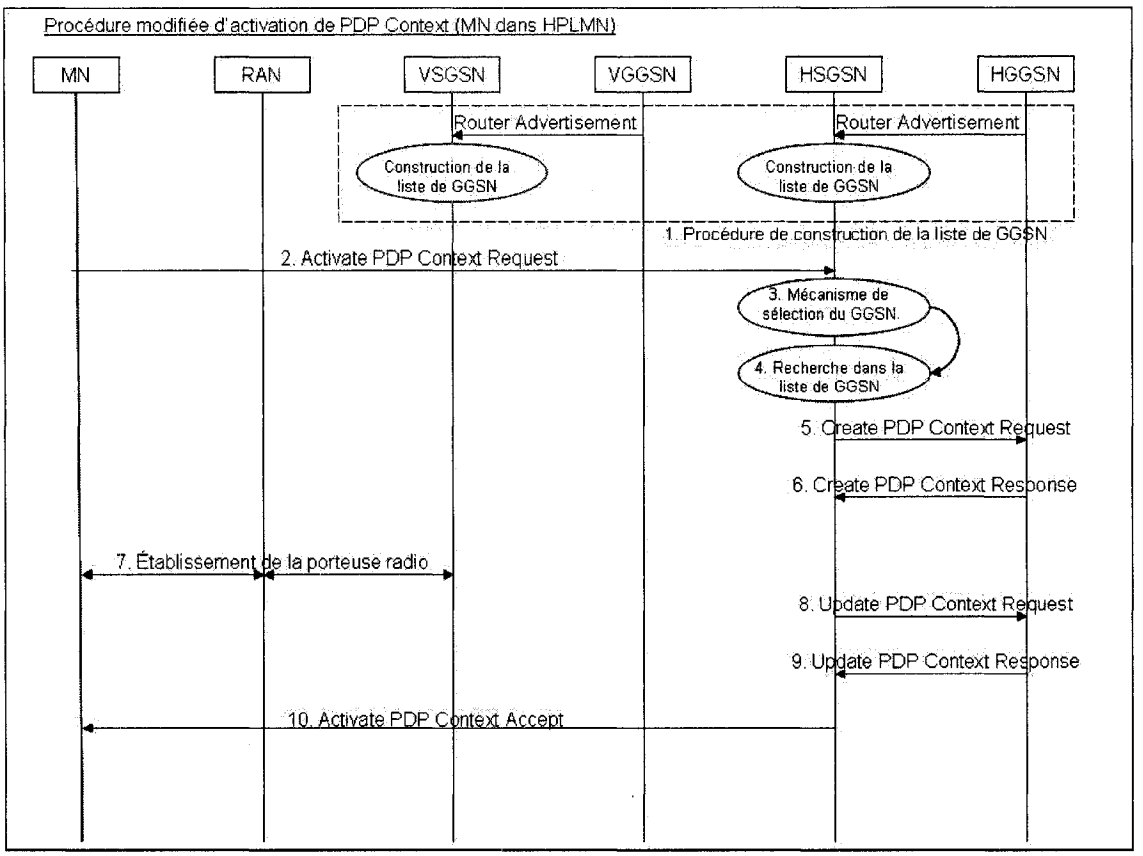


Figure 3.4 Diagramme de messages "1er scénario"

1. La procédure de construction de la liste de GGSN est effectuée de façon périodique et non sollicitée indépendamment de la procédure d'activation de *PDP Context*. Cependant, il est impératif qu'elle ait eu lieu au moins une fois avant le déclenchement de la procédure d'activation de *PDP Context* pour éviter un échec de celle-ci ;
2. Le MN envoie un message *Activate PDP context request* au SGSN de son PLMN d'origine (HSGSN). C'est un message de signalisation contenant plusieurs paramètres nécessaires à la mise en œuvre du mécanisme de sélection du GGSN tels que : le *ServiceID*, le PDP Type, l'adresse PDP. Après réception du message, le HSGSN vérifie l'enregistrement de l'abonnement de l'usager pour établir la validité de la requête ;

3. Par la suite, le HSGSN applique le mécanisme de sélection du GGSN. Dans ce scénario, quel que soit le mode de sélection du *ServiceID*, le PLMN du GGSN choisi sera forcément le PLMN d'origine du MN ;
4. Une fois en possession de toutes les informations dont il a besoin, le HSGSN lance une recherche dans sa liste de GGSN qui devrait aboutir à l'obtention de l'adresse IP du GGSN capable de fournir le service désiré par le MN. Si aucun GGSN n'est trouvé dans la liste alors la requête d'activation de *PDP Context* est rejetée ;
5. Le HSGSN envoie un message *Create PDP context request* au HGGSN dont l'adresse a été obtenue à l'issue de la recherche dans la liste de GGSN. Le HGGSN crée une nouvelle entrée dans sa table de *PDP contexts* qui lui permettra de router les paquets entre le HSGSN et le réseau PDN ;
6. Le GGSN retourne un message *Create PDP context response* au HSGSN. Si le HGGSN est responsable de l'allocation de la *PDP address*, celle-ci est incluse dans le message. Sinon, le champ correspondant est mis à 0.0.0.0 indiquant ainsi que c'est au MN de négocier une *PDP address* avec un PDN externe après la complétion de la procédure ;
7. Une procédure d'établissement de la porteuse de l'accès radio est entreprise. Elle peut entraîner une modification à la baisse de la QoS ;
8. et 9. Si les paramètres de QoS ont été modifiés, le HSGSN et le HGGSN échangent la paire de messages *Update PDP context request* et *Update PDP context response* afin de modifier en conséquence ces paramètres dans le *PDP context* ;
9. Le HSGSN envoie un message *Activate PDP context Accept* au MN pour conclure la procédure.

Hormis l'étape 1, ce sont les étapes 2, 3 et 4 qui concentrent les principales modifications apportées à la procédure d'activation de *PDP Context*. Les étapes

subséquentes restent inchangées, aussi nous ne répéterons pas leur description dans la suite.

Dans les trois prochains scénarii, l'usager mobile MN se trouve dans un PLMN visité.

- Le deuxième scénario de la Figure 3.4 s'attache à décrire un échange de messages efficace en cas de *roaming*. En effet, le MN utilise ici les services du PLMN visité évitant ainsi les délais qui auraient été introduits par un échange de messages avec un GGSN de son réseau d'origine.

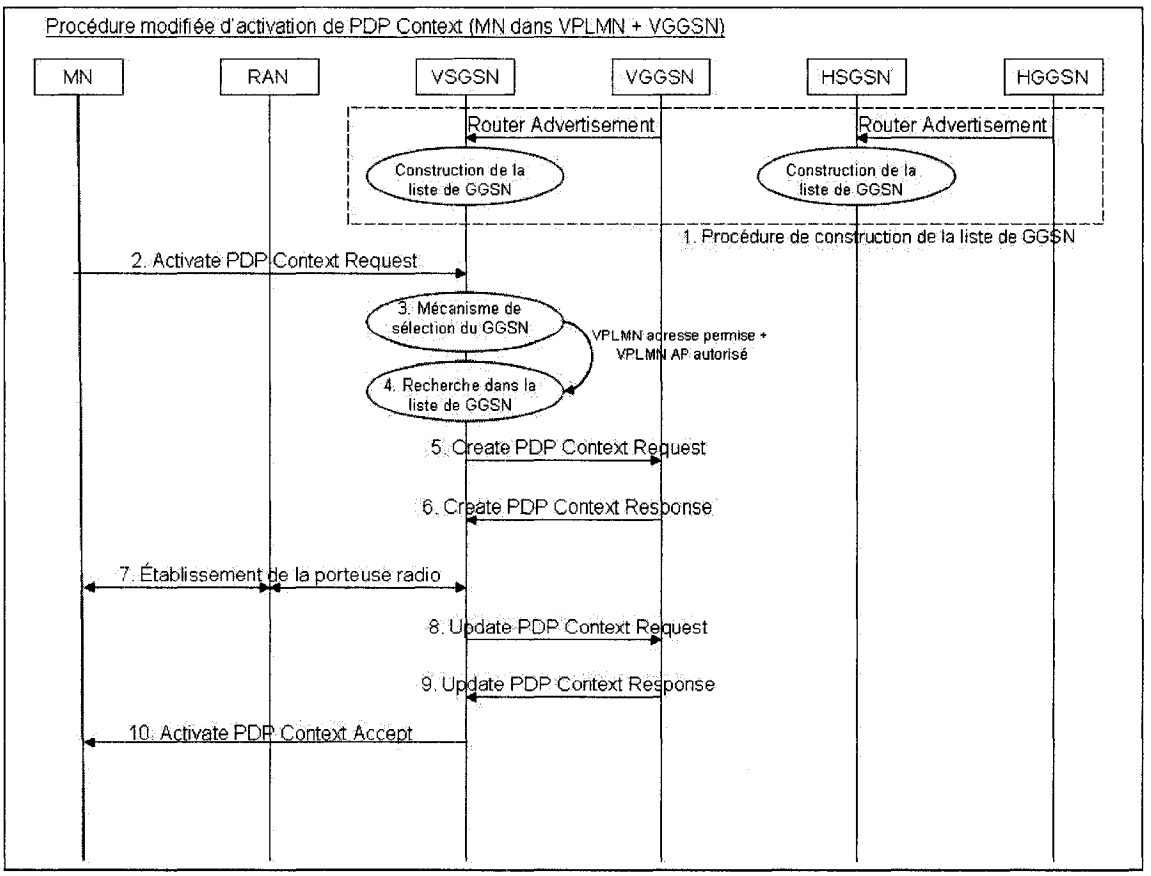


Figure 3.5 Diagramme de messages "2e scénario"

1. (est la même que pour le scénario 1) ;
2. Le MN envoie un message *Activate PDP context request* au SGSN du PLMN dans lequel il se trouve. Puisqu'il est en *roaming*, c'est un SGSN du réseau visité (VSGSN) qui le prend en charge. Par la suite, le VSGSN vérifie l'enregistrement de l'abonnement de l'usager pour établir la validité de la requête. Cette étape reste la même pour tous les scénarii de *roaming* donc pour les scénarii 2, 3 et 4 ;
3. Une fois établie la validité de la requête du MN, le VSGSN applique le mécanisme de sélection du GGSN. Ce sont les résultats de l'application du mécanisme qui distinguent chacun des scénarii de *roaming*. Dans ce scénario-ci, le MN a le droit d'utiliser les services du PLMN visité (VPLMN adresse permise) et l'accès au point d'accès du PLMN visité lui est également autorisé. Toutes les conditions sauf une sont réunies pour qu'un VGGSN serve le MN ;
4. La dernière condition à satisfaire est de trouver l'adresse du VGGSN susceptible de fournir le service dont le *ServiceID* a été sélectionné. Le VSGSN lance donc une recherche dans sa liste de GGSN. Si aucun GGSN n'est trouvé, la requête d'activation de *PDP Context* est alors rejetée. Sinon, la procédure d'activation de *PDP Context* se poursuit.

C'est donc l'occurrence de ce scénario que nous voulons faire tendre vers 100% en cas de *roaming*. En utilisant les services d'un GGSN local et en supprimant la paire de messages liée à l'interrogation du serveur DNS, certains délais n'entrent plus en ligne de compte et ne pénalisent plus la procédure d'activation du *PDP Context*.

Les deux derniers scénarii partagent la même étape 2 avec le précédent scénario.

- Le troisième scénario illustré à la Figure 3.5 correspond aux échanges de messages de deux cas différents.

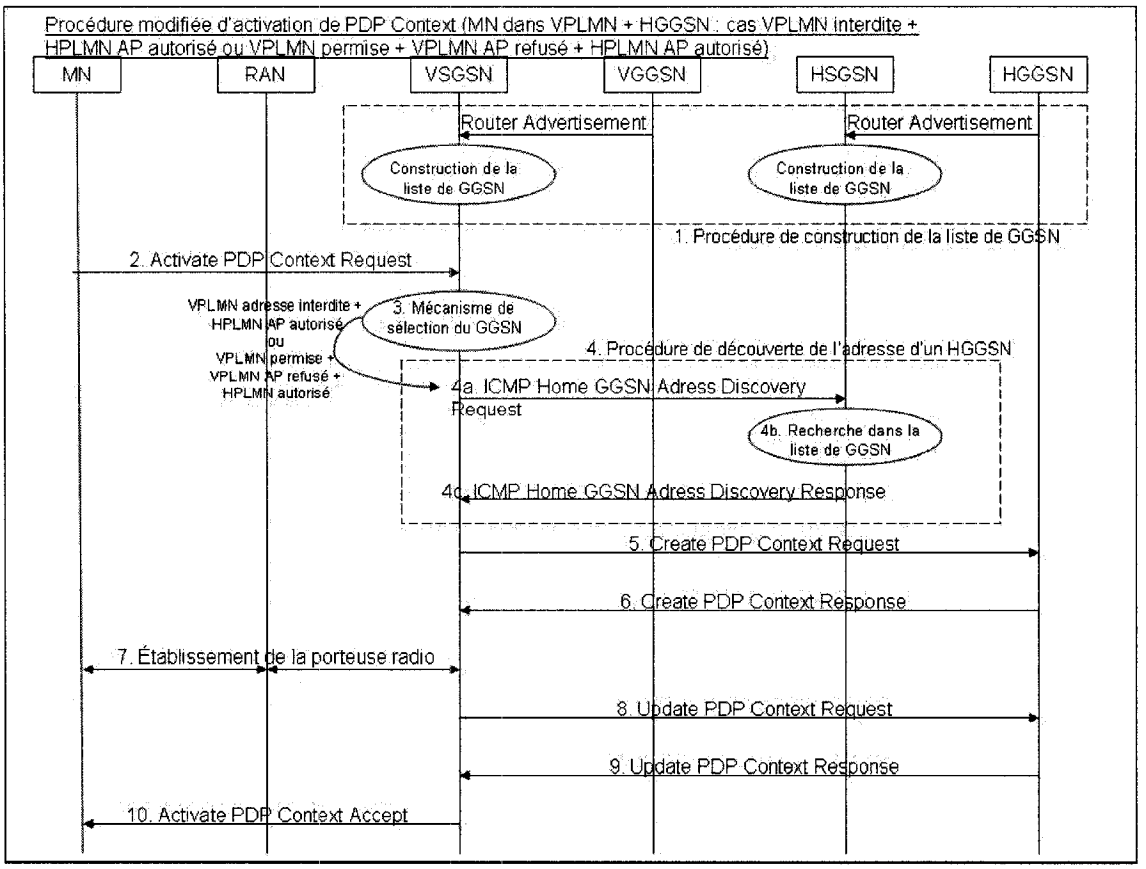


Figure 3.6 Diagramme de messages "3e scénario"

1. et 2. (sont les mêmes que pour le scénario précédent) ;
3. Comme nous l'avons mentionné un peu plus haut, ce sont les résultats de l'application du mécanisme de sélection du GGSN qui distinguent chacun des scénarii de *roaming*. Le troisième scénario fait référence à deux situations différentes même si le choix du PLMN se porte sur le réseau d'origine dans les deux cas. Ainsi, l'échange de messages de la Figure 3.3 aura lieu si le MN n'a pas le droit d'utiliser les services du réseau visité (VPLMN adresse interdite) ou alors s'il possède ce droit mais que l'accès au point d'accès du VPLMN lui est refusé. Dans les deux cas, il faut que l'accès au point d'accès du PLMN d'origine soit autorisé ;

4. Le choix du PLMN s'étant porté sur le réseau d'origine du MN, le VSGSN doit donc obtenir l'adresse d'un GGSN du PLMN d'origine. Il lance la procédure de découverte de l'adresse IP du HGGSN qui elle-même se divise en trois étapes :
    a) Le VSGSN envoie un message *ICMP Home GGSN Address Discovery Request* contenant le *ServiceID* sélectionné à l'adresse unicast des SGSN du PLMN d'origine du MN ;
    b) Le message parvient à un SGSN du PLMN d'origine qui effectue la recherche dans sa liste de GGSN avec comme clé le *ServiceID* du message ;
    c) Le message *ICMP Home GGSN Address Discovery Response* retourné au VSGSN contient en principe l'adresse IP du GGSN trouvée dans la liste ou un message d'erreur. Si aucune adresse de GGSN n'a été trouvée, la procédure d'activation de *PDP Context* est rejetée. Dans le cas contraire, elle se poursuit avec les étapes subséquentes de la procédure.

Enfin, concluons avec le dernier et aussi le plus long scénario illustré à la Figure 3.6 :

1. et 2. (sont les mêmes que dans le scénario précédent) ;
3. La situation qui prévaut dans ce scénario est celle pour laquelle le MN possède le droit d'utiliser les services du PLMN visité ainsi que l'autorisation d'accéder au point d'accès du VPLMN mais où la recherche dans la liste des GGSN du VSGSN se solde par un échec (étape 4.1). Dans ce cas, le choix du PLMN qui s'est d'abord porté sur le réseau visité sans succès se fixe sur le PLMN d'origine du MN ;
4. Comme dans le scénario précédent, le VSGSN lance donc la procédure de découverte de l'adresse IP du HGGSN dont la réussite ou l'échec entraînera

respectivement la poursuite ou le rejet de la procédure d'activation du *PDP Context.*

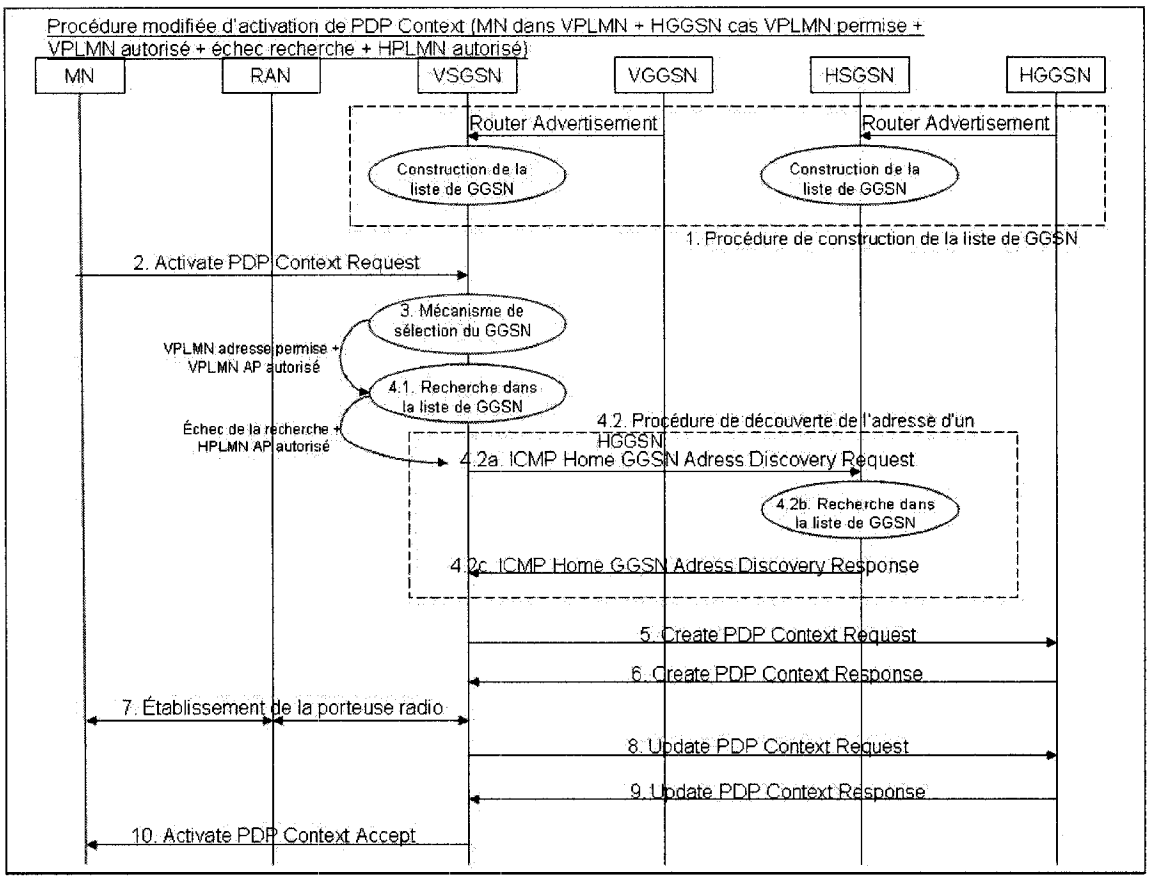


Figure 3.7 Diagramme de messages "4e scénario"

Les deux derniers scénarii constituent, en quelque sorte, des scénarii de secours dont l'occurrence est minimisée par les deux hypothèses énoncées précédemment :

- La majorité des usagers ont le droit d'utiliser les services d'un PLMN autre que le leur ;

- Les PLMNs qui permettent à leurs usagers d'utiliser leurs services respectifs doivent s'assurer qu'un ensemble de GGSN ou un GGSN fournit les services proposés par son pair.

La première hypothèse adresse le problème du troisième scénario, tandis que la seconde solutionne celui du quatrième.

En tous les cas, la mise en œuvre de cette procédure modifiée d'activation de *PDP Context* doit conduire à la résolution du problème d'ancrage géographique dû à l'APN lors du *roaming* d'un usager mobile.

3.2.7 Autres changements à apporter

Le *PDP Context* est la structure de données au cœur des préoccupations de ce mémoire. Et pour cause, c'est grâce à elle que le GGSN servant un usager mobile gère le routage et le transfert des paquets en provenance ou à destination du réseau de données pour ce dernier. Différentes procédures manipulent le *PDP Context* :

- La procédure d'activation de *PDP Context* ;
- La procédure d'activation de *PDP Context* secondaire ;
- La procédure de modification de *PDP Context* ;
- La procédure de désactivation de *PDP Context* ;

Cependant, l'accent a été mis sur la procédure d'activation de *PDP Context* car c'est la seule qui détermine la valeur de l'APN. Or ce sont les délais introduits par l'ancrage géographique dû à l'APN que ce mémoire tente d'éliminer. Afin d'atteindre cet objectif, nous avons apporté certaines modifications à la procédure d'activation de *PDP Context*. Le changement le plus marquant en ce qui a trait aux répercussions est celui du remplacement de l'APN par le *ServiceID*. En pratique, dans les procédures manipulant le *PDP Context*, il suffit de faire un simple échange entre les deux entités sans autre artifice.

Un remplacement est également nécessaire dans toutes les structures de données dans le MN, le SGSN, le GGSN, le HLR, etc. qui possèdent un champ APN ou relié à l'APN tel que *APN subscribed* ou encore *APN in use.*

L'APN est aussi utilisé dans le processus de facturation pour identifier les différents services. Le remplacement ne devrait en principe causer aucun problème puisque la vocation du *ServiceID* est de classer les services. Néanmoins, une analyse plus approfondie hors du cadre de ce mémoire permettrait de s'en assurer de façon formelle.

CHAPITRE 4
ÉVALUATION DE PERFORMANCE

Dans le chapitre précédent, nous avons présenté en détail notre mécanisme d'abolition de l'ancrage géographique de l'APN. Le principe de ce dernier consiste à remplacer l'*Access Point Name* par le *ServiceID*, un identifiant capable de désigner de façon unique un réseau de données ou un service. Puisque le *ServiceID* n'est pas un nom conforme au DNS comme l'APN, ce remplacement nécessite la création de procédures telles que la construction de la liste de GGSN et la découverte de l'adresse IP d'un *Home* GGSN afin d'assurer la correspondance entre le *ServiceID* et l'adresse IP du GGSN auquel il fait référence. Dans ce chapitre, nous commençons par valider notre mécanisme d'abolition avec le logiciel UPPAAL puis nous nous livrons à une estimation des délais occasionnés par ce mécanisme.

4.1 Présentation générale de l'outil de validation utilisé

Cette section est consacrée à l'analyse par le logiciel UPPAAL des différents mécanismes que nous avons conçus. Cette analyse nous permettra d'effectuer une vérification formelle de notre système afin de nous assurer de sa fiabilité et de la cohérence de ses fonctionnalités. Nous pourrons également vérifier que le comportement du système est bien conforme à celui attendu et qu'il possède bien les propriétés prévues dans les spécifications. Cependant, avant de commencer cette analyse, intéressons-nous au logiciel UPPAAL et à son fonctionnement.

Le logiciel UPPAAL est un environnement de modélisation, de simulation et de vérification de systèmes temps réels mis au point par les universités Uppsala en Suède et Aalbord au Danemark. L'utilisation d'UPPAAL comporte quatre étapes distinctes :

- La modélisation, étape de construction d'un modèle de vérification formelle ;
- La simulation, étape de validation et de raffinement du modèle construit ;
- La spécification des propriétés, étape d'énonciation des propriétés à vérifier ;
- La vérification, étape de vérification des propriétés avec le moteur de vérification.

Pour UPPAAL, un modèle consiste en un ensemble d'automates temporisés, qui communiquent par une synchronisation binaire, utilisant des canaux et une syntaxe du type émission/réception. Ainsi, sur le canal c, un émetteur envoie le signal c ! et un récepteur se synchronise avec lui par le signal complémentaire c ?. Les automates temporisés d'UPPAAL sont des structures finies manipulant deux types de variables : des horloges, qui évoluent de manière synchrone avec le temps, et des variables entières discrètes bornées. Un état de l'automate peut comporter une condition sur les horloges, appelée *invariant*, qui doit être satisfaite pendant toute la durée passée dans cet état. Une transition de l'automate est étiquetée par :

- une *garde*, qui exprime une condition sur les valeurs des variables (true par défaut). Cette condition doit généralement être compatible avec l'invariant de l'état origine de la transition et elle doit être satisfaite pour franchir la transition ;
- une *synchronisation* de la forme c ! ou c ?, l'absence de synchronisation indiquant une action interne de l'automate ;
- une *remise à zéro* de certaines horloges et une mise à jour de certaines variables entières.

Une configuration (globale) du système est une paire (l ; v) ou l (pour location) est un vecteur indiquant l'état de chacun des automates et v est une évaluation des variables. Une exécution est une suite de configuration qui part d'un état initial de chacun des automates avec toutes les valeurs des variables à zéro. La sémantique de ce modèle contient trois types de changements de configurations (ou mouvements) :

- Délai : le temps peut progresser dans les états courants d'une durée *d*, à condition que l'invariant de chacun de ces états reste satisfait. Les valeurs des horloges augmentent de *d* et les valeurs des variables discrètes ne changent pas ;
- Synchronisation : Si deux actions complémentaires de deux composants sont possibles, et que les gardes associées aux transitions sont satisfaites, ces deux composants se synchronisent. Les états correspondants sont modifiés, et les valeurs des horloges et des variables discrètes sont modifiées selon les indications de remises à zéro et de mises à jour ;
- Action interne : Si une action interne (sans synchronisation) d'un composant est possible (sa garde est satisfaite), cette action peut être exécutée indépendamment des autres composants : l'état et les variables du composant sont modifiés comme dans le cas précédent.

Cette description non exhaustive d'UPPAAL améliorera la compréhension du modèle de notre système présenté dans la sous section suivante.

4.2. Validation des mécanismes proposés

Cette section est entièrement dédiée à la description des étapes du processus de validation et à la présentation des résultats obtenus. Nous commençons tout d'abord par présenter notre modèle et les propriétés que nous désirons vérifier. Puis, nous achevons avec une discussion des résultats.

4.2.1 Description du modèle

Notre modèle de vérification formelle comporte cinq automates temporisés :

- Un automate UE représentant l'usager mobile ;
- Un automate SGSN représentant les nœuds SGSN dans les réseaux d'origine et visité ;

- Un automate GGSN représentant les nœuds GGSN dans les réseaux d'origine et visité ;
- Un automate RAN représentant le nœud de l'accès radio (*Radio Access Node*) ;
- Un automate SelectionGGSN représentant le mécanisme de sélection du GGSN.

L'automate UE est illustré à la Figure 4.1. Il possède un paramètre *location* qui peut prendre deux valeurs. Lorsque sa valeur est 1, cela signifie que l'usager mobile est dans son réseau d'origine tandis que la valeur 2 indique que l'usager se trouve dans un réseau visité.

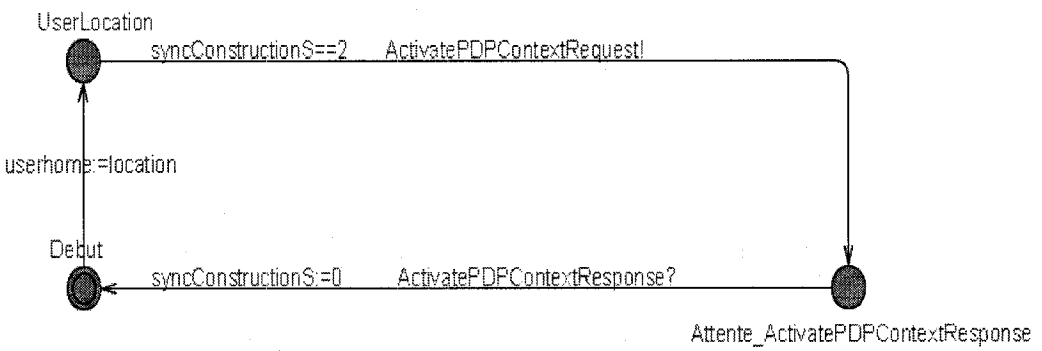


Figure 4.1 Automate UE

L'automate UE possède deux transitions étiquetées par les synchronisations *ActivatePDPContextRequest !* et *ActivatePDPContextResponse ?* qui en encadrent l'état *Attente_ActivatePDPContextResponse.* L'automate demeure dans cet état jusqu'à la fin de la demande d'activation de PDP Context qui débute avec l'envoi du message *ActivatePDPContextResquest* et qui prend fin avec la réception du *ActivatePDPContextResponse.*

L'automate SGSN est illustré à l'Annexe 1. Il s'agit de l'automate le plus complexe du modèle. D'ailleurs, pour en faciliter la compréhension, le mécanisme de

sélection du GGSN qui est pourtant effectué par le SGSN a été modélisé dans un autre automate, SelectionGGSN.

Les SGSN du réseau d'origine et du réseau visité possèdent des comportements similaires. Aussi, nous avons modélisé un patron de SGSN et seul le paramètre *location* distingue un *Home SGSN* d'un *Visited SGSN*. Comme pour l'automate UE, une valeur de 1 du paramètre *location* indique que le SGSN est dans le réseau d'origine et une valeur de 2 qu'il se trouve dans le réseau visité.

Peu importe sa localisation, tout SGSN effectue la procédure de construction de la liste de GGSN. Cette dernière est modélisée par la transition étiquetée entre autres par la synchronisation *HrouterAdvertisement ?* pour le HSGSN et *VrouterAdvertisement ?* pour le VSGSN et par l'état *ConstructionListeGGSN*. Par la suite, le SGSN tombe dans l'état *Idle*. Les états suivants sont alors entièrement fonction de la localisation de l'usager mobile. En effet, ce dernier est servi par le SGSN qui se trouve dans le même réseau que lui. Aussi, le SGSN qui ne sert pas l'usager mobile demeure dans l'état *Idle* tandis que l'autre passe dans l'état *Ready* dans lequel il attend le début de la demande d'activation de PDP Context. La procédure d'activation de PDP Context standard est constituée d'un ensemble d'états et de transitions étiquetées par des synchronisations qui modélisent l'échange de messages entre le SGSN de service, le GGSN choisi, le RAN et le UE. Il est toutefois intéressant de noter qu'une fois arrivé dans l'état *Reception_ActivatePDPContextRequest*, le mécanisme de sélection du GGSN est effectué par l'automate approprié. Une fois la sélection terminée, le SGSN de service reprend le contrôle.

Enfin, la procédure de découverte de l'adresse IP du HGGSN s'effectue entre le VSGSN qui initie la procédure et le HSGSN. L'automate SGSN modélise donc les comportements des deux parties impliquées dans ladite procédure. Le comportement du VSGSN, SGSN de service, est représenté par les états *Attente_ICMPHGGSNAddressDiscoveryResponse* et *FinProcedureDecouverteHGGSN* et par les transitions étiquetées par les synchronisations

ICMPHGGSNAddressDiscoveryRequest ! et *ICMPHGGSNAddressDiscoveryresponse ?*. Le comportement du HGGSN, en revanche, est modélisé par l'état *Reception_ICMPHGGSNAddressDiscoveryRequest* et par les transitions étiquetées par les synchronisations *ICMPHGGSNAddressDiscoveryRequest ?* et *ICMPHGGSNAddressDiscoveryResponse !*.

L'automate GGSN est illustré à la Figure 4.2. Cet automate, tout comme celui du SGSN, est un *template* dont le paramètre *location* permet de distinguer les comportements de HGGSN et de VGGSN.

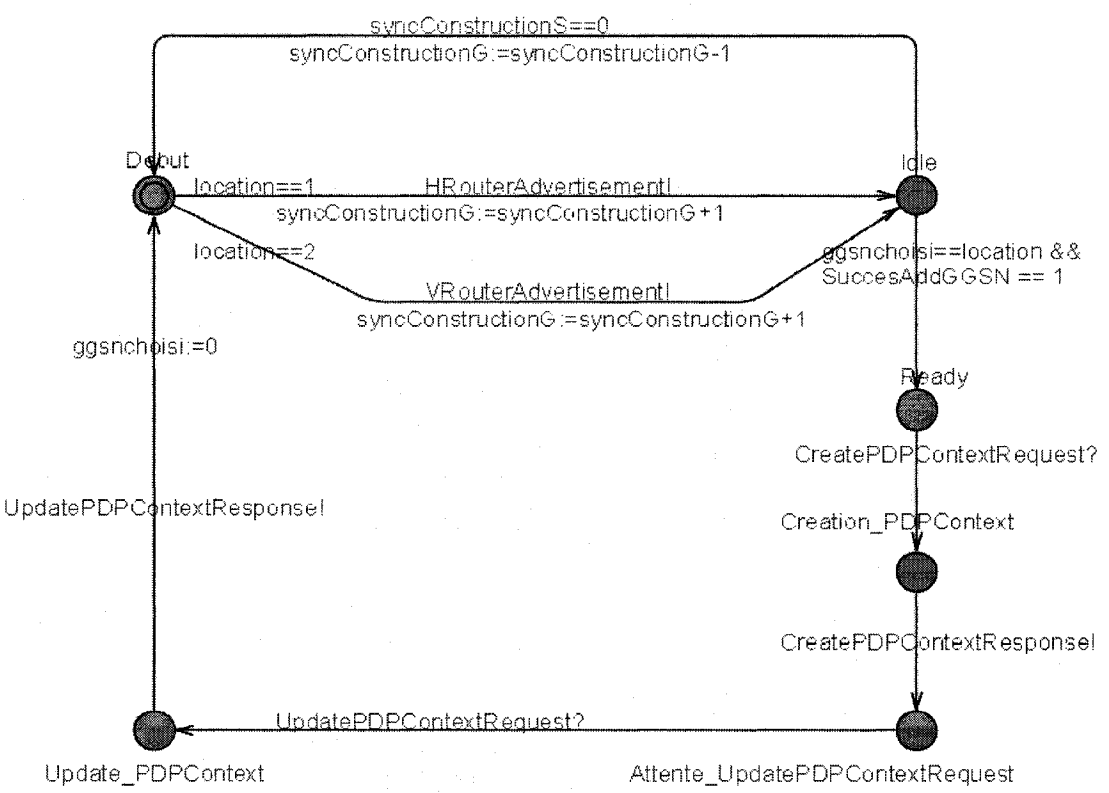


Figure 4.2 Automate du GGSN

Ici encore, peu importe sa localisation, le GGSN effectue la procédure de construction de la liste de GGSN avant de tomber dans l'état *Idle*. La dite procédure

est modélisée par la transition étiquetée par les synchronisations *HRouterAdvertisement !* pour le HGGSN et *VRouterAdvertisement !* pour le VGGSN.

Une fois dans l'état *Idle*, les états suivants de l'automate dépendent du résultat du mécanisme de sélection du GGSN. Seul le GGSN du réseau sélectionné passe à l'état *Ready* et continue l'activation du PDP Context.

L'automate RAN est représenté à la Figure 4.3. Il ne présente aucun intérêt particulier puisque nous n'avons rien modifié à son comportement.

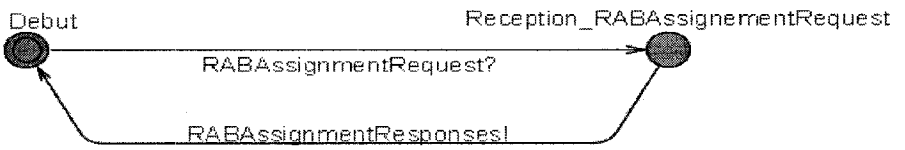


Figure 4.3 Automate du RAN

L'automate SelectionGGSN est illustré à l'Annexe 2. Ce dernier modélise le mécanisme de sélection du GGSN. Cet automate prend le contrôle aussitôt que l'automate SGSN atteint l'état *Reception_ActivatePDPContextRequest.* Il possède quatre paramètres qui permettent de distinguer les différents scénariis : *rechercheroaming, vplmnadd, vplmap, hplmnap.*

Chacun des paramètres est un booléen. *Rechercheroaming* indique la présence ou l'absence du *ServiceID* sélectionné dans la liste de GGSN dans le réseau visité. Le paramètre *vplmnap* montre si l'accès au point d'accès du réseau visité est autorisé ou non tandis que *hplmnap* en fait de même pour le réseau d'origine. Enfin, *vplmnadd* signale si l'usager mobile est autorisé à utiliser les services d'un GGSN du réseau visité.

Le mécanisme de sélection du GGSN se distingue par le remplacement de l'APN par le *ServiceID*, celui de la requête au serveur DNS par la recherche dans la liste de GGSN et par la procédure de découverte de l'adresse IP du HGGSN. La

recherche dans la liste de GGSN est ici modélisée par les transitions étiquetées par la garde *rechercheroaming*==*Y*. La procédure de découverte de l'adresse IP du HGGSN, quant à elle, est modélisée par l'état *ProcédureDecouverteHGGSN* et les transistions étiquetées par *ProcedureHGGSN :=1* et *ProcedureHGGSN ==2* qui l'encadrent. Dès que l'automate *SelectionGGSN* atteint l'état *ProcedureDecouverteHGGSN*, l'automate *SGSN*, qui modélise le VSGSN, prend le contrôle afin de poursuivre la procédure. Une fois, cette dernière achevée du côté du VSGSN, le mécanisme de sélection du GGSN reprend où il s'était arrêté.

Nous avons achevé la description des automates de notre modèle. Si on assimile ces automates aux classes de la programmation orientée objet, nous venons de définir nos classes. À présent, nous devons instancier nos objets. Du point de vue des automates, il s'agit de l'assignation des processus (*Process Assignment*). C'est à ce moment que nous pouvons déterminer les différents scénarii à étudier en attribuant les valeurs appropriées des paramètres. Un exemple d'assignation de processus est présenté ci-après :

```
MU :=UE(0) ;
HSGSN :=SGSN( 1) ;
VSGSN:=SGSN(2) ;
HGGSN:=GGSN(1) ;
VGGSN:=GGSN(2) ;
RAN1:=RAN() ;
Selecteur:=SelectionGGSN(0,1,1,1) ;
```

Nous avons identifié les scénarii d'intérêt pour notre étude. Nous allons les décrire.

Scénario 1

Valeurs des paramètres :

```
UE.location = 1
Selecteur.rechercheroaming = 0/1
Selecteur.vplmnadd = 0/1
Selecteur.vplmnap = 0/1
Selecteur.hplmnap = 0/1
```

Ce scénario illustre le cas où l'usager mobile est dans son réseau d'origine. Ici, le seul paramètre pertinent est *UE.location* qui indique la position de l'usager. Nous avons écarté le scénario dans lequel le *ServiceID* sélectionné est absent de ladite liste car il n'est pas réaliste. En effet, il n'est pas concevable qu'un usager demande des services que son propre réseau n'est pas en mesure de lui fournir.

Scénario 2

Valeurs des paramètres :

```
UE.location = 2
Selecteur.rechercheroaming = 0/1
Selecteur.vplmnadd = 0
Selecteur.vplmnap = 0/1
Selecteur.hplmnap = 0
```

Comme l'indique le paramètre *UE.location*, dans ce scénario, l'usager mobile se trouve dans un réseau visité. Par ailleurs, la seconde information d'intérêt est fournie par *Selecteur.vplmnadd* qui nous apprend que l'usager mobile n'est pas autorisé à utiliser les services d'un VGGSN. Aussi, la seule alternative est d'essayer d'utiliser les services d'un HGGSN or le paramètre *Selecteur.hplmnap* nous informe que l'accès au point d'accès du réseau d'origine n'est pas autorisé.

Scénario 3

Valeurs des paramètres :

```
UE.location = 2
Selecteur.rechercheroaming = 0/1
Selecteur.vplmnadd = 0
Selecteur.vplmnap = 0/1
Selecteur.hplmnap = 1
```

Le scénario 3 va de paire avec le scénario 2. Dans ce dernier, l'usager mobile en roaming ne peut accéder ni aux services du réseau visité ni à ceux de son réseau d'origine. Le scénario 3, en revanche, a un paramètre *Selecteur.hplmnap* dont la valeur autorise l'accès au réseau d'origine. Le *ServiceID* sélectionné existe dans la liste de GGSN du réseau d'origine. Encore une fois, nous avons écarté le cas où le *ServiceID* sélectionné serait absent de la liste de GGSN du réseau d'origine de l'usager mobile.

Scénario 4

Valeurs des paramètres :

```
UE.location = 2
Selecteur.rechercheroaming = 0/1
Selecteur.vplmnadd = 1
Selecteur.vplmnap = 0
Selecteur.hplmnap =0
```

Dans ce scénario, l'usager mobile en roaming a l'autorisation d'utiliser les services d'un VGGSN mais, comme l'indique les paramètres *Selecteur.vplmnap* et *Selecteur.hplmap*, il n'a accès ni au point d'accès du réseau visité ni à celui du réseau d'origine.

Scénario 5

Valeurs des paramètres :

```
UE.location = 2
Selecteur.rechercheroaming = 0/1
Selecteur.vplmnadd = 1
Selecteur.vplmnap = 0
Selecteur.hplmnap =1
```

Le scénario 5 va de paire avec le précédent mais contrairement à ce dernier, l'usager mobile en roaming a accès au point d'accès du réseau d'origine comme l'indique la valeur du paramètre *Selecteur.hplmnap* et le *ServiceID* sélectionné appartient à la liste de GGSN du réseau d'origine.

Scénario 6

Valeurs des paramètres :

```
UE.location = 2
Selecteur.rechercheroaming = 0
Selecteur.vplmnadd = 1
Selecteur.vplmnap = 1
Selecteur.hplmnap =0
```

Dans ce scénario, l'usager mobile en roaming a l'autorisation d'utiliser les services d'un VGGSN et il a également accès au point d'accès du réseau visité mais comme le montre la valeur du paramètre *Selecteur.rechercheroaming*, le *ServiceID* sélectionné est absent de la liste de GGSN du réseau visité. La seule alternative est

d'essayer d'utiliser les services d'un HGGSN or le paramètre *Selecteur.hplmnap* nous informe que l'accès au point d'accès du réseau d'origine n'est pas autorisé.

Scénario 7

Valeurs des paramètres :

```
UE.location = 2
Selecteur.rechercheroaming = 0
Selecteur.vplmnadd = 1
Selecteur.vplmnap = 1
Selecteur.hplmnap =1
```

Ce scénario va de paire avec le précédent mais contrairement à ce dernier, la valeur du paramètre *Selecteur.hplmap* indique que l'usager mobile en roaming a accès au point d'accès du réseau d'origine et le *ServiceID* sélectionné existe dans la liste de GGSN du réseau d'origine.

Scénario 8

Valeurs des paramètres :

```
UE.location = 2
Selecteur.rechercheroaming = 1
Selecteur.vplmnadd = 1
Selecteur.vplmnap = 1
Selecteur.hplmnap =0/1
```

Il s'agit du scénario dont nous souhaitons augmenter l'occurrence. Dans celui-ci, l'usager mobile en roaming a l'autorisation d'utiliser les services d'un VGGSN et il a également accès au point d'accès du réseau visité. Enfin, comme l'indique le paramètre *Selecteur.rechercheroaming*, le *ServiceID* sélectionné existe dans la liste de GGSN du réseau visité.

Avec cette description des scénarii à analyser, nous terminons la présentation de notre modèle de vérification sur le logiciel UPPAAL. Nous pouvons donc passer à l'étape de vérification.

4.2.2 Vérification du modèle

Dans cette sous-section, nous livrons les résultats de la vérification formelle du modèle. Nous avons tout d'abord énoncé les propriétés d'intérêts selon le langage *Computational Tree Logic* (CTL). Par la suite, nous avons utilisé le serveur de vérification de UPPAAL pour nous assurer que ces propriétés sont satisfaites.

Les propriétés ont été regroupées en différentes catégories : les propriétés de vivacité, les propriétés de sureté, les propriétés de survivabilité et de disponibilité, les propriétés d'intégrité et de cohérence.

Les propriétés de vivacité stipulent qu'un état bien déterminé doit être atteint à partir d'un autre état si des conditions sont satisfaites. Elles permettent de valider le comportement du modèle. Dans cette catégorie, nous citons les propriétés suivantes :

- Résultat d'une requête d'activation de PDP Context :

Cette propriété se lit : il est toujours vrai qu'un HSGSN (respectivement un VSGSN) ne se retrouve jamais simultanément dans les états *Echec_ActivatePDPContext* (échec de la requête) et *Fin_Update_PDPContext* (succès de la requête).

```
A[] not (HSGSN.Echec_ActivatePDPContext and HSGSN.Fin_Update_PDPContext)
A[] not (VSGSN.Echec_ActivatePDPContext and VSGSN.Fin_Update_PDPContext)
```

- Lorsque l'usager est dans son réseau d'origine, le GGSN choisi est toujours dans son réseau d'origine :

La propriété se lit : il est toujours vrai que lorsque le mécanisme de sélection du GGSN s'achève (état *HSGSN.FinSelectionGGSN*) et que l'usager est son réseau d'origine (*userhome==1*), le GGSN sélectionné se trouve dans le réseau d'origine de l'usager (*ggsnchoisi==1*).

```
A[] HSGSN.FinSelectionGGSN and userhome==1 imply ggsnchoisi==1
```

- Résultat du mécanisme de sélection du GGSN :

  Les propriétés se lisent ainsi :

  - Il est toujours vrai que si le mécanisme de sélection du GGSN est achevé (*finSelection==1*) alors soit une adresse IP de GGSN a été trouvée (*succesAddGGSN==1*) ou non (*succesAddGGSN==0*) ;
  - Il est toujours vrai que si une adresse IP de GGSN n'a pas été trouvée et que le mécanisme de sélection du GGSN est achevé alors la localisation du GGSN reste indéterminée (*ggsnchoisi==0*) ;
  - Il est toujours vrai que si un adresse IP de GGSN a été trouvée et que mécanisme de sélection du GGSN est achevé alors la localisation du GGSN est soit le réseau d'origine soit le réseau visité.

```
A[] finSelection==1 imply (SuccesAddGGSN==0 or SuccesAddGGSN==1)
A[] SuccesAddGGSN==0 and finSelection==1 imply ggsnchoisi==0
A[] SuccesAddGGSN==1 and finSelection==1 imply (ggsnchoisi==1 or ggsnchoisi==2)
```

Les propriétés de sureté indiquent que, sous certaines conditions, quelque chose n'arrivera jamais.

- Aucune requête d'activation de PDP Context ne peut être envoyée avant que les listes de GGSNs soient construites :

La propriété se lit : il est toujours vrai que si le HSGSN (respectivement le VSGSN) reçoit le message d'activation du PDP Context alors la construction des listes de GGSN est complétée dans les réseaux d'origine et visité.

```
A[] HSGSN.Reception_ActivatePDPContextRequest imply syncConstructionS==2
A[] VSGSN.Reception_ActivatePDPContextRequest imply syncConstructionS==2
```

- La procédure de découverte de l'adresse IP du HGGSN ne peut débuter avant que les listes de GGSNs soient construites :

La propriété se lit : il est toujours vrai que si le VSGSN est en attente de la réponse de son message *ICMP HGGSN Address Discovery Request* (début de la

procédure de découverte de l'adresse IP du HGGSN) alors la construction des listes de GGSN est complétée dans les réseaux d'origine et visité.

```
A[] VSGSN.AttenteICMPHGGSNAddressDiscoveryResponse imply syncConstructionS==2
```

En ce qui concerne les propriétés de disponibilité et de survivabilité, nous ne citerons que la propriété suivante :

- Le protocole ne bloque jamais :

```
A[] not deadlock
```

Les propriétés d'intégrité et de cohérence permettent d'assurer que le système ne pourra jamais induire en erreur.

- Si l'usager communique avec un SGSN alors ce dernier se trouve dans le même réseau que lui :

La propriété se lit ainsi : il est toujours vrai que si un HSGSN (respectivement un VSGSN) reçoit un message *Activate PDP Context Request* du MU alors l'usager se trouve dans le réseau d'origine (respectivement le réseau visité).

```
A[] HSGSN.Reception_ActivatePDPContextRequest imply userhome==1
A[] VSGSN.Reception_ActivatePDPContextRequest imply userhome==2
```

- Si un GGSN sert l'usager alors il a été choisi par le mécanisme de sélection du GGSN :

La propriété se lit : il est toujours vrai que si un HGGSN (respectivement un VGGSN) sert l'usager alors le mécanisme de sélection du GGSN s'est achevé en le sélectionnant.

```
A[] HGGSN.Ready imply ggsnchoisi==1 and finSelection==1
A[] VGGSN.Ready imply ggsnchoisi==2 and finSelection==1
```

- La procédure de découverte de l'adresse IP d'un HGGSN s'effectue entre 2 SGSN de réseaux différents :

La propriété se lit : il est toujours vrai que si le HSGSN reçoit un message *ICMP HGGSN Address Discovery Request* alors le VSGSN est en attente du message de réponse *ICMP HGGSN Address Discovery Response.*

```
A[] VSGSN.AttenteICMPHGGSNAddressDiscoveryResponse imply
HSGSN.ReceptionICMPHGGSNAddressDiscoveryRequest
```

- Si la procédure de découverte de l'adresse IP d'un HGGSN a lieu, alors l'usager se trouve dans un réseau visité :

```
A[] procedureHGGSN==1 imply userhome==2
```

- Si la procédure de découverte de l'adresse IP d'un HGGSN a lieu, alors aucun VGGSN ne peut servir l'usager :

La propriété se lit ainsi : si aucun VGGSN ne peut servir l'usager (interdiction d'accéder au service du réseau visité, interdiction d'accès au point d'accès du réseau visité, absence du *ServiceID* dans la liste de GGSN du réseau visité), alors la procédure de découverte de l'adresse IP d'un HGGSN a lieu.

```
A[] procedureHGGSN==1 imply (Selecteur.vplmnadd==0 and Selecteur.hplmnap==1)
or (Selecteur.vplmnadd==1 and Selecteur.vplmnap==0 and Selecteur.hplmnap==1)
or (Selecteur.rechercheroaming==0 and Selecteur.vplmnadd==1 and
Selecteur.vplmnap==1 and Selecteur.hplmnap==1)
```

4.2.3 Synthèse de la validation

À l'aide du *model-checker* du logiciel UPPAAL, nous avons pu vérifier les propriétés énumérées ci-dessus. Cela nous a permis de nous assurer du bon fonctionnement du modèle conçu. Ainsi, toutes les propriétés attendues du système ont pu être validées de même que le comportement escompté de ce dernier.

Ainsi, les propriétés de vivacité garantissent que le modèle réagit bien comme prévu dans des situations bien déterminées. Ainsi, lorsqu'une demande d'activation

de PDP Context est initiée, elle reçoit obligatoirement une réponse qu'elle soit positive ou négative. Il en va de même pour le mécanisme de sélection du GGSN.

En ce qui concernent les propriétés de sureté, elles assurent qu'aucune situation indésirable ne sera rencontrée. Dans cette optique, nous avons la certitude que les listes de GGSN ne seront jamais indisponibles au moment où elles sont nécessaires durant la procédure de découverte de l'adresse IP du HGGSN ou la demande d'activation de PDP Context.

L'unique propriété de disponibilité et de survivabilité a également été la première à être tester. Elle fait la preuve que le modèle est à l'abri de toute situation de blocage.

La dernière catégorie de propriétés fait partie des plus importantes. En effet, l'intégrité et la cohérence du modèle est cruciale. À présent, nous sommes assurés que le mécanisme d'abolition de l'ancrage géographique de l'APN ne nous induira en erreur d'aucune façon.

Notre modèle a été validé selon différents aspects. Nous avons donc l'assurance qu'il fonctionne correctement. Il s'agit à présent de vérifier qu'il remplit bien les objectifs de performance escomptés.

4.3 Analyse de performance

La section précédente a été consacrée à la validation formelle du mécanisme proposé. Cette dernière adressait surtout le comportement du mécanisme. En ce qui concerne les améliorations attendues, cependant, la vérification formelle ne nous est d'aucun secours. En effet, dans la forme, tant l'APN que le *ServiceID* permettent à un usager mobile en visite dans un réseau étranger d'utiliser les services d'un GGSN local. Cette section a pour but d'estimer les bénéfices du mécanisme proposé en gardant à l'esprit l'objectif principal de ce mémoire : proposer un mécanisme capable de réduire les délais liés à l'ancrage géographique de l'*Access Point Name*.

4.3.1 Les indices de performance

Afin de mettre en évidence les apports des mécanismes que nous avons mis au point, nous allons procéder à une évaluation de performance. Cette dernière se déroule en plusieurs étapes dont la première est la définition des indices de performance. Ceux-ci, comme leur nom l'indique, nous renseigne sur la manière dont le système évalué s'acquittent de ses fonctions. Ils permettent de quantifier la performance du système mais également de le comparer avec d'autres sur des bases équivalentes.

La réalisation de cette première étape de l'évaluation de performance nous a conduit à dégager trois indices pertinents pour nos mécanismes d'abolition de l'ancrage dynamique de l'APN :

- Le délai moyen d'une communication de l'usager ;
- Le temps moyen d'exécution des mécanismes ;
- Le nombre moyen de requêtes traitées avec succès.

Le délai moyen d'une communication de l'usager constitue l'indice le plus significatif puisqu'il est directement relié à l'objectif principal de ce mémoire. En effet, les délais que nous nous proposons de réduire par la conception d'un mécanisme approprié sont justement ceux qui se produisent lorsqu'un usager en *roaming* communique avec un autre. La comparaison de cet indice de performance avec celui du système actuel basé sur l'APN nous indiquera donc si nous avons atteint ou non notre objectif en matière de performance.

Les mécanismes que nous avons proposés agissent essentiellement au niveau de la procédure d'activation de *PDP Context* car c'est la seule et unique procédure qui permet de choisir le GGSN en charge du transfert et du routage des paquets pour l'usager mobile. Une fois, ce GGSN sélectionné, il n'existe aucun moyen de le modifier et tout le trafic pour l'usager mobile et en provenance de ce dernier doit

passer par l'élu. Malgré cela, pour l'estimation du délai moyen de la communication, la procédure d'activation, elle-même, n'entre pas en ligne de compte. Seuls les scénarii pertinents et les résultats qu'ils produisent nous intéressent. Ainsi, à la fin de la procédure d'activation de *PDP Context*, peu importe le scénario, trois situations peuvent se présenter :

- La requête d'activation est rejetée ;
- Le *PDP Context* a été établi avec un HGGSN ;
- Le *PDP Context* a été établi avec un VGGSN.

Parmi ces trois situations, seules les deux dernières ont un intérêt pour nous. Les Figures 4.4 et 4.5 illustrent la première tandis que la Figure 4.6 illustre la deuxième situation.

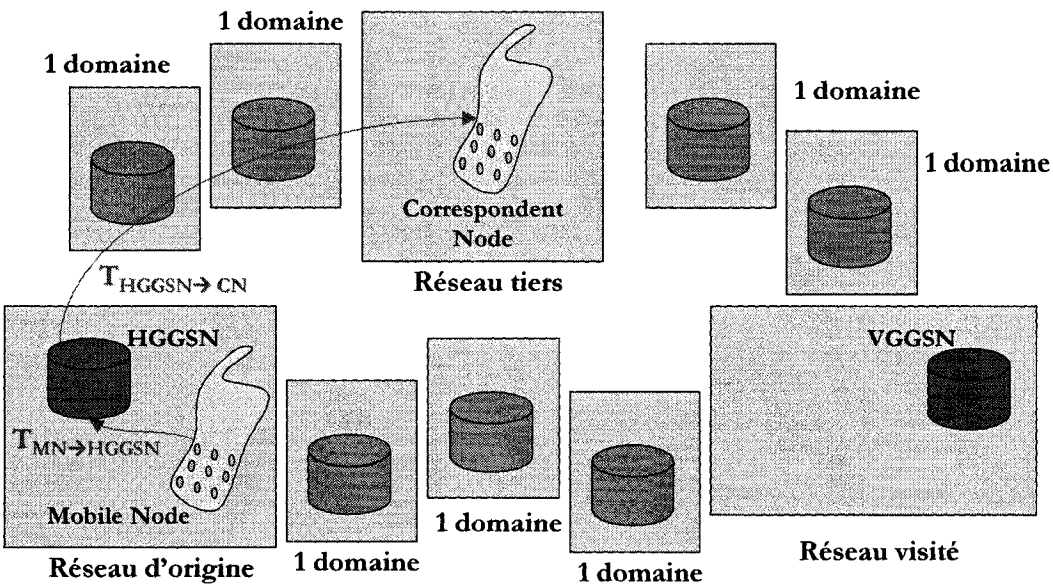


Figure 4.4 Situation 1 : appel de l'usager à domicile géré par le réseau d'origine

Pour chaque situation, le délai subi par le trafic de l'usager durant la communication peut être estimé. Ainsi, nous pouvons exprimer le délai moyen de la

communication comme la somme pour tous les scénarii du produit de la probabilité d'occurrence du scénario par le délai subi par le trafic de l'usager pour ce scénario :

$$\Sigma_i^{nb\_scénarii} P_{scénario} \times Délai_{scénario}$$

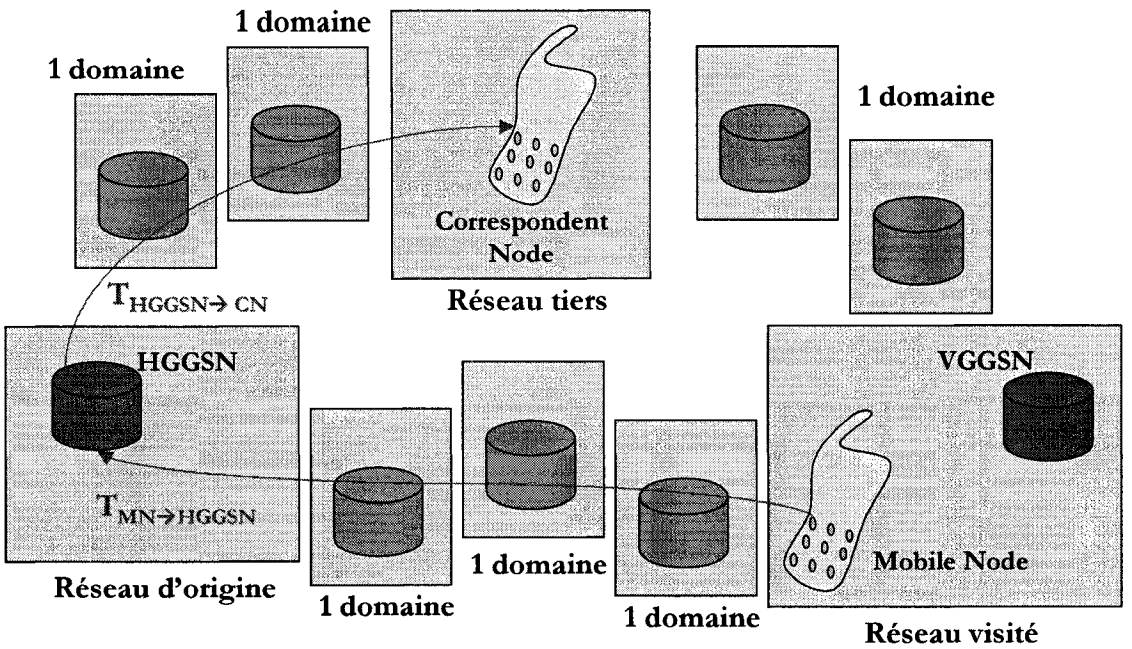


Figure 4.5 Situation 1 : appel de l'usager en *roaming* géré par le réseau d'origine

En premier lieu, nous allons définir les quatre scénarii pertinents pour notre analyse :

- Scénario 1 : l'usager se trouve dans son réseau d'origine et est servi par un HGGSN ;
- Scénario 2 : l'usager se trouve dans un réseau visité et est servi par un VGGSN ;
- Scénario 3 : l'usager se trouve dans un réseau visité et est servi par un HGGSN car certaines autorisations lui ont été refusées ;

- Scénario 4 : l'usager se trouve dans un réseau visité et est servi par un HGGSN car le *ServiceID* sélectionné est absent de la liste de GGSN du réseau visité.

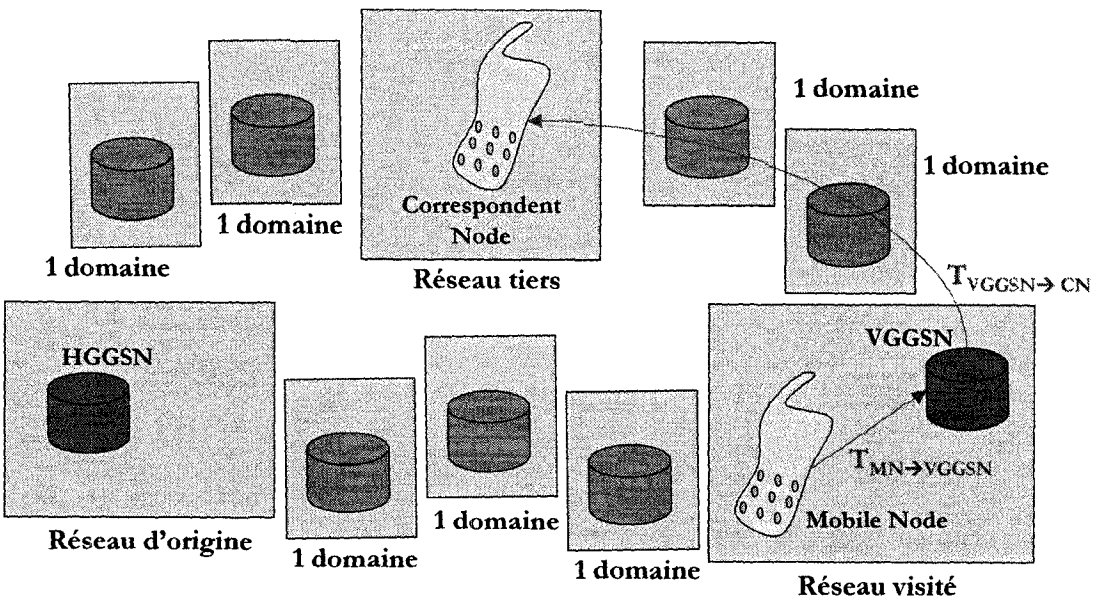


Figure 4.6 Situation 2 :appel de l'usager en *roaming* géré par le réseau visité

À présent, nous pouvons déterminer les délais subis par l'usager durant sa communication associé à chaque scénario, soit $Délai_1$, $Délai_2$, $Délai_3$, $Délai_4$. Après une brève analyse, nous avons pu établir que les scénarii 3 et 4 possèdent la même valeur de délai subi par l'usager durant sa communication puisque dans les deux cas, l'usager en *roaming* est servi par un HGGSN. Nous avons donc trois valeurs à définir.

Considérons le scénario 1 dans lequel le *PDP Context* de l'usager à domicile est établi avec un HGGSN. Le délai maximal subi par le trafic de l'usager peut être exprimé comme la somme de deux termes :

$$Délai_1 = (T_{MN \rightarrow HGGSN})_{home} + T_{HGGSN \rightarrow CN}$$

Il est en de même pour le scénario 2 :

$$Délai_2 = T_{MN \rightarrow VGGSN} + T_{VGGSN \rightarrow CN}$$

Ainsi que pour les scénarii 3 et 4 :

$$Délai_3 = Délai_4 = (T_{MN \rightarrow HGGSN})_{visited} + T_{HGGSN \rightarrow CN}$$

Pour simplifier le calcul, on pose l'hypothèse que le temps nécessaire pour que le message soit transféré du VGGSN au CN ($T_{VGGSN \rightarrow CN}$) est le même que celui nécessaire pour passer du HGGSN au CN ($T_{HGGSN \rightarrow CN}$). Autrement dit, le CN est à égale distance des GGSNs des réseaux d'origine et visité en termes de délai :

$$T_{HGGSN \rightarrow CN} = T_{VGGSN \rightarrow CN}$$

De plus, afin de nous aider à déterminer les trois composantes de délai restantes, examinons la Figure 4.7.

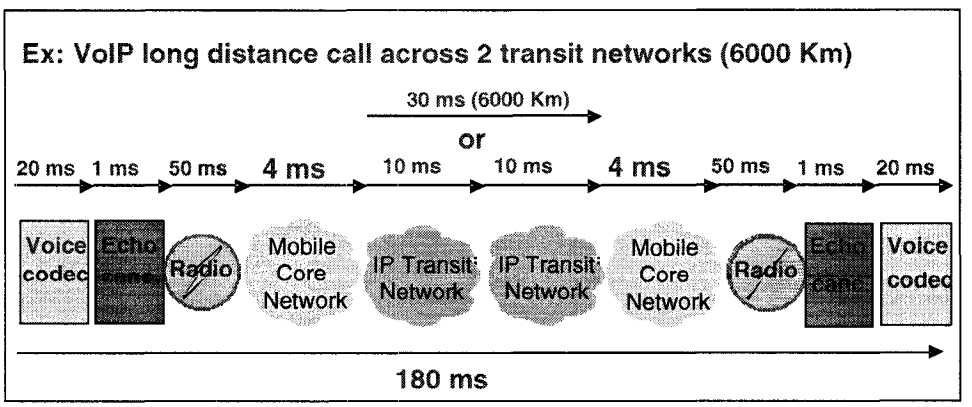


Figure 4.7 Requis de qualité de service bout en bout

Elle nous permet de décomposer les composantes de délai. Ainsi, $(T_{MN \rightarrow HGGSN})_{home}$ est composé :

- Du temps pour la compression par un codec de voix ;
- Du temps pour l'annulation de l'écho ;
- Du temps de transmission radio ;
- Du temps nécessaire pour atteindre le GGSN dans le réseau cœur UMTS.

$$(T_{MN \rightarrow HGGSN})_{home} = 20 + 1 + 50 + 4 = 74 \text{ ms}$$

On obtient donc un temps maximal de transmission entre le nœud mobile et le HGGSN de 74 ms. On procède de la même manière avec $T_{MN \rightarrow VGGSN}$ et $(T_{MN \rightarrow HGGSN})_{visited}$.

$$T_{MN \rightarrow VGGSN} = 20 + 1 + 50 + 4 = 74 \text{ ms}$$

On constate que les deux temps $(T_{MN \rightarrow HGGSN})_{home}$ et $T_{MN \rightarrow VGGSN}$ sont égaux. C'est logique puisque dans les deux cas, le GGSN utilisé se trouve dans le même réseau que l'usager. Cependant, pour $(T_{MN \rightarrow HGGSN})_{visited}$, l'usager et le GGSN se trouve dans des réseaux différents. Aussi, on ajoute aux composantes de temps citées précédemment le temps nécessaire pour traverser trois domaines IP de transit. En effet, on estime qu'en moyenne trois domaines de transit séparent les réseaux intercontinentaux.

$$(T_{MN \rightarrow HGGSN})_{visited} = 20 + 1 + 50 + 4 + 3*10 = 104 \text{ ms}$$

On obtient alors un temps maximal de transmission entre le nœud mobile et le HGGSN de 104 ms. Enfin, évaluons les composantes de délai $T_{HGGSN \rightarrow CN}$ et $T_{VGGSN \rightarrow CN}$:

$$T_{HGGSN \rightarrow CN} = T_{VGGSN \rightarrow CN} = 4 + 2*10 + 50 + 1 + 20 = 95 \text{ ms}$$

Ainsi, nous obtenons les délais suivants :

$$\mathbf{Délai_1 = Délai_2 = 74 + 95 = 169 \text{ ms}}$$

$$\mathbf{Délai_3 = Délai_4 = 104 + 95 = 199 \text{ ms}}$$

Les derniers éléments manquants pour pouvoir évaluer l'expression du délai moyen de la communication sont les probabilités d'occurrence de chaque scénario, soit P_1, P_2, P_3, P_4. Ces dernières expriment la probabilité que le mécanisme de sélection du GGSN aboutisse aux résultats associés à chaque scénario.

Ainsi, P_1 correspond à la probabilité que l'usager soit dans son réseau d'origine et que le mécanisme de sélection du GGSN choisisse un HGGSN :

$$\mathbf{P_1 = P_{Home}}$$

En effet, la probabilité que le mécanisme de sélection du GGSN choisisse un HGGSN sachant que l'usager est dans son réseau d'origine est égale à 1.

En ce qui concerne P_2, il s'agit de la probabilité que l'usager soit dans un réseau visité et que le mécanisme de sélection du GGSN choisisse un VGGSN. Cette probabilité est reliée à :

- La probabilité que l'usager soit dans le réseau visité : P[!Home]=1-P[Home] = 1-PHome ;
- La probabilité que l'usager ait l'autorisation d'utiliser les services du réseau visité : P[VPLMNAd] ;
- La probabilité que l'usager ait accès au point d'accès du réseau visité : P[VPLMNAP] ;
- La probabilité que le *ServiceID* sélectionné soit dans la liste de GGSN du réseau visité : P[Liste].

On peut donc exprimer P_2 de la manière suivante :

$$P_2 = P[\ !Home \cap VPLMNAd \cap VPLMNAP \cap Liste\ ]$$

La liste d'hypothèses suivantes va nous aider à évaluer cette probabilité :

- On connaît la probabilité que le *ServiceID* sélectionné soit dans la liste de GGSN du réseau visité sachant que la probabilité que l'usager a l'autorisation d'utiliser les services du réseau visité : P[Liste | VPLMNAd] = X (1) ;
- On connaît la probabilité que l'usager ait accès au point d'accès du réseau visité sachant que la probabilité que l'usager a l'autorisation d'utiliser les services du réseau visité : P[VPLMNAP | VPLMNAd] = Y (2) ;
- La probabilité que le *ServiceID* sélectionné soit dans la liste de GGSN du réseau visité sachant que la probabilité que l'usager a l'autorisation d'utiliser les services du réseau visité et que l'usager a accès au point d'accès du réseau visité est égale à celle que le *ServiceID* sélectionné soit dans la liste de GGSN du réseau visité sachant que la probabilité que l'usager a l'autorisation

d'utiliser les services du réseau visité : P[Liste | VPLMNAd ∩ VPLMNAP] = P[Liste | VPLMNAd] (3) ;

- L'événement Home est indépendant de chacun des événements suivants : VPLMNAd, VPLMAP et Liste (4);

À partir de ces hypothèses, nous pouvons déduire que :

(1) → P[Liste ∩ VPLMNAd] = X * $P_{VPLMNAd}$; (*)

(2) → P[VPLMNAP ∩ VPLMNAd] = Y * $P_{VPLMNAd}$; (**)

(3) → P[Liste ∩ VPLMNAd ∩ VPLMNAP] = P[Liste | VPLMNAd] * P[VPLMNAP ∩ VPLMNAd] ; (***)

(**) et (***) → P[Liste ∩ VPLMNAd ∩ VPLMNAP] = X * Y * $P_{VPLMNAd}$; (****)

(4) → P_2 = P[!Home] * P[VPLMNAd ∩ VPLMNAP ∩ Liste] ; (*****)

(****) et (*****) → P_2 = (1-P_{Home}) * X * Y * $P_{VPLMNAd}$;

Nous obtenons donc l'expression de la probabilité P_2 :

$$\mathbf{P_2 = (1\text{-}P_{Home}) * X * Y * P_{VPLMNAd}}$$

Nous poursuivons notre analyse avec la probabilité P_3 que l'usager soit dans un réseau visité et que le mécanisme de sélection du GGSN choisisse un HGGSN car certaines autorisations ont été refusées. Procédons comme précédemment en exprimant P_3 :

$$P_3 = P[(!Home \cap !VPLMNAd \cap HPLMNAP) \cup (!Home \cap VPLMNAd \cap !VPLMNAP \cap HPLMNAP)]$$

Cette probabilité correspond à la réunion de deux événements incompatibles (qui ne peuvent se produire en même temps). On peut en déduire l'expression suivante :

$$P_3 = P[!Home \cap !VPLMNAd \cap HPLMNAP] + P[!Home \cap VPLMNAd \cap !VPLMNAP \cap HPLMNAP]$$

Aux hypothèses émises précédemment, nous ajoutons celles-ci pour aider à l'évaluation de la probabilité P_3 :

- Les événements Home, VPLMNAd et HPLMNAP sont indépendants deux à deux (5) ;
- Les événements Home, VPLMNAP et HPLMNAP sont indépendants deux à deux (6).

On déduit de ces hypothèses :

(5) et (6) → P_3 = P[!Home]*P[!VPLMNAd]*P[HPLMNAP] +
P[!Home]*P[VPLMNAd ∩ !VPLMNAP]*P[HPLMNAP] ; (#)
P[!VPLMNAd |VPLMNAd] = 1- P[VPLMNAd |VPLMNAd] = 1-Y ; (##)
(##) → P[VPLMNAd ∩ !VPLMNAP] = (1-Y)* $P_{VPLMNAd}$; (###)
(#) et (###) → $P_3 = (1-P_{Home})* (1-P_{VPLMNAd})* P_{HPLMNAP}$ +
$(1-P_{Home})* (1-Y)*P_{VPLMNAd} * P_{HPLMNAP}$

Nous obtenons donc l'expression de la probabilité P_3 :

$$\mathbf{P_3 = (1-P_{Home})* P_{HPLMNAP}*(1-Y*P_{VPLMNAd})}$$

Nous terminons avec la probabilité P_4 que l'usager soit dans un réseau visité et que le mécanisme de sélection du GGSN choisisse un HGGSN car le *ServiceID* est absent de la liste de GGSN du réseau visité :

P_4 = P[!Home ∩ VPLMNAd ∩ VPLMNAP ∩ !Liste ∩ HPLMNAP]

L'hypothèse suivante permet de simplifier notre expression :

- Les événements Liste et HPLMNAP sont indépendants (7).

On peut faire les déductions suivantes :

(5), (6) et (7) → P_4 =P[!Home]*P[VPLMNAd∩VPLMNAP∩ !Liste]
*P[HPLMNAP] ; ($)
P[!Liste |VPLMNAd ∩ VPLMNAP] = 1-P[Liste |VPLMNAd ∩ VPLMNAP] ; ($$)
(3), (***) et ($$) → P[VPLMNAd∩VPLMNAP∩ !Liste] = (1-X)*Y*$P_{VPLMNAd}$; ($$$)
($) et ($$$) → $P_4 = (1-P_{Home})*(1-X)*Y* P_{VPLMNAd} * P_{HPLMNAP}$.

Nous obtenons donc l'expression de P_4 :

$$\mathbf{P_4 =(1-P_{Home})*(1-X)*Y* P_{VPLMNAd} * P_{HPLMNAP}}$$

Nous avons à présent tous les éléments pour évaluer l'indice de performance, délai moyen de la communication de l'usager pour les mécanismes proposés. Nous avons exécuté un travail similaire pour obtenir l'expression du même indice de performance mais pour le système actuel basé sur l'APN. L'expression général du délai moyen de la communication de l'usager reste la même tout comme les scénarii utilisés et les valeurs des $Délai_{scénario}$. Seules les expressions des probabilités $P_{scénario}$ changent. Les détails des calculs sont présentés en annexe. On obtient les expressions suivantes :

$$(P_1)_{APN} = P_{Home}\,(1 + (W-1)*P_{APN\text{-}OI} + (1-W)*P_{APN\text{-}OI}*P_{APNSGSN})$$

$$(P_2)_{APN} = (1-P_{Home})*Z*P_{VLMNAd}*[((1-W)+ (W-1)*P_{DNS})*P_{APN\text{-}OI} + ((W-1)+(1-W)*P_{DNS})*P_{APN\text{-}OI}*P_{APNSGSN} + P_{APNSGSN} + P_{DNS} - P_{APNSGSN}*P_{DNS}]$$

$$(P_3)_{APN}=(1-P_{Home})*P_{HPLMNAP}*[(1-P_{APN\text{-}OI})*(1-P_{VPLMNAd})+(1-P_{APN\text{-}OI})*Z*P_{VLMNAd}+(1-W)*P_{APN\text{-}OI}]$$

$$(P_4)_{APN} = (1-P_{Home})*Z*P_{VLMNAd}*(1-P_{DNS})$$

Le temps moyen d'exécution des mécanismes est l'indice de performance qui évalue nos mécanismes en eux-mêmes. En effet, ce temps moyen n'influe pas directement sur la qualité de service d'une communication de l'usager. L'exécution de la procédure d'activation de PDP *context* ne se produit qu'une fois lorsque l'usager allume son mobile ou lorsqu'il entre dans le réseau visité pour la première fois. Ainsi, ce temps d'exécution des mécanismes n'ajoute ni n'enlève rien au délai moyen de la communication de l'usager. Cependant, il est judicieux de s'assurer que cette exécution n'est pas excessivement longue (de l'ordre de plusieurs secondes). Ici encore, cet indice de performance est fonction des scénarii pertinents. Il s'exprime comme la somme pour tous les scénarii du produit de la probabilité d'occurrence d'un scénario par le temps d'exécution des mécanismes pour ce scénario :

$$\Sigma_i^{nb\_scénarii}\, P_{scénario} \times Temps_{scénario}$$

Nous avons déjà déterminé la valeur des probabilités $P_{scénario}$ précédemment. Aussi, nous n'aurons à définir que les temps d'exécution des différents scénarii qui restent les mêmes que ceux de l'indice du délai moyen de la communication de l'usager. Chaque temps d'exécution peut être décomposé de la façon suivante :

$T_1 = T_{ConstructionListe} + 2*T_{ActivateMsg} + T_{Mécanisme} + T_{Recherche} + 2*(T_{CreateMsg})_{1Réseau} + T_{CreateProcess} + T_{PorteuseRadio} + 2*(T_{UpdateMsg})_{1Réseau} + T_{UpdateProcess}$

$T_2 = T_{ConstructionListe} + 2*T_{ActivateMsg} + T_{Mécanisme} + T_{Recherche} + 2*(T_{CreateMsg})_{1Réseau} + T_{CreateProcess} + T_{PorteuseRadio} + 2*(T_{UpdateMsg})_{1Réseau} + T_{UpdateProcess}$

$T_3 = T_{ConstructionListe} + 2*T_{ActivateMsg} + T_{Mécanisme} + 2*T_{ICMPHGGSNMsg} + T_{Recherche} + 2*(T_{CreateMsg})_{2Réseaux} + T_{CreateProcess} + T_{PorteuseRadio} + 2*(T_{UpdateMsg})_{2Réseaux} + T_{UpdateProcess}$

$T_4 = T_{ConstructionListe} + 2*T_{ActivateMsg} + T_{Mécanisme} + T_{Recherche} + 2*T_{ICMPHGGSNMsg} + T_{Recherche} + 2*(T_{CreateMsg})_{2Réseaux} + T_{CreateProcess} + T_{PorteuseRadio} + 2*(T_{UpdateMsg})_{2Réseaux} + T_{UpdateProcess}$

Encore une fois, grâce à la Figure 4.8, nous pouvons établir des valeurs maximales pour les composantes des différents temps d'exécution :

$$T_{ConstructionListe} = 4 + 1 = 5 \text{ ms}$$

$$T_{Mécanisme} = T_{Recherche} = T_{CreateProcess} = T_{UpdateProcess} = 1 \text{ ms}$$

$$(T_{CreateMsg})_{1Réseau} = (T_{UpdateMsg})_{1Réseau} = 4 \text{ ms}$$

$$T_{ActivateMsg} = 50 + 4 + 1 = 55 \text{ ms}$$

$$(T_{CreateMsg})_{2Réseaux} = (T_{UpdateMsg})_{2Réseaux} = T_{ICMPHGGSNMsg} = 4 + 3*10 + 4 = 38 \text{ ms}$$

$$T_{PorteuseRadio} = 4 + 50 + 1 + 50 + 4 = 109 \text{ ms}$$

Nos calculs se fondent sur l'hypothèse que l'exécution de tous les mécanismes et processus ne dépassera pas 1 ms. Ainsi, on obtient les temps d'exécution des scénarii suivants :

$T_1 = 5 + 2*55 + 1 + 1 + 2*4 + 1 + 109 + 2*4 + 1 = 244$ ms

$T_2 = 5 + 2*55 + 1 + 1 + 2*4 + 1 + 109 + 2*4 + 1 = 244$ ms

$T_3 = 5 + 2*55 + 1 + 2*38 + 1 + 2*38 + 1 + 109 + 2*38 + 1 = 456$ ms

$T_4 = 5 + 2*55 + 1 + 1 + 2*38 + 1 + 2*38 + 1 + 109 + 2*38 + 1 = 457$ ms

Nous procédons de la même façon pour obtenir l'expression du temps d'exécution pour le système actuel basé sur l'APN. Encore une fois, l'expression générale reste inchangée et les probabilités sont les $(P_{scénario})_{APN}$ déterminées précédemment. Seuls les temps d'exécution du mécanisme de sélection de l'APN pour chaque scénario, $(T_{scénario})_{APN}$, sont à définir. Les détails des calculs sont présentés en annexe. Nous obtenons les valeurs suivantes :

$(T_1)_{APN} = (T_2)_{APN} = 244$ ms

$(T_3)_{APN} = 304$ ms

$(T_4)_{APN} = 312$ ms

Enfin, le dernier indice de performance, le nombre de requêtes traitées avec succès, nous renseigne sur l'efficacité de nos mécanismes. Il fait partie des paramètres de qualité de service observables. Cet indice a également l'avantage de permettre une comparaison avec les mécanismes actuels basés sur l'APN. Il est intimement lié au mécanisme de sélection du GGSN ou au mécanisme de sélection de l'APN. En effet, dans la majorité des cas, c'est lors de l'exécution de ces mécanismes que le résultat de la requête d'activation est déterminé. Les quatre scénarii décrits et analysés précédemment correspondent également les seuls qui aboutissent au succès de la requête d'activation de PDP *Context*. On en déduit donc que l'expression du pourcentage de requêtes traitées avec succès est :

$$\sum_i^{nb\_scénarii} P_{scénario}$$

Les probabilités $P_{scénario}$ sont celles que nous avons déterminées précédemment. L'expression de cet indice est la même pour le système basé sur l'APN à l'exception que les probabilités sont $(P_{scénarion})_{APN}$.

4.3.2 Paramètres et plan d'expérience

La sous-section précédente a permis d'accomplir la première étape de notre analyse de performance : définir les indices de performance. Nous poursuivons donc avec la seconde étape. Cette sous-section est consacrée à la détermination des paramètres des expériences que nous allons mener ainsi qu'à la conception du plan d'expérience. Ces paramètres sont de deux natures :

- Les facteurs ;
- Le type d'expérience à mener.

Les facteurs qui peuvent être quantitatifs ou non, sont des paramètres susceptibles d'influencer de façon substantielle les valeurs des indices de performance. Les valeurs de ces facteurs sont appelés « niveaux ». Une session est une combinaison bien particulière de niveaux de facteurs tandis qu'une expérience peut être composée de plusieurs sessions. Aussi, la conception d'une expérience passe par l'identification des facteurs et au choix de leurs niveaux pour chaque session.

La sous-section précédente a déjà déblayé le terrain. En effet, la détermination des expressions des différents indices de performance a mis en évidence les éléments qui influencent ces derniers. La liste suivante énumère ceux du mécanisme d'abolition de l'APN et ceux du système actuel basé sur l'APN :

- PHome ;
- PVPLMNAd ;
- PHPLMNAP ;
- P[Liste | VPLMNAd] = X ;
- P[VPLMNAP | VPLMNAd] = Y ;
- PAPN-OI ;
- PDNS ;
- P[HAPN-OI | APN-OI] = Z ;

- P[VPLMNAP | VPLMNAd]APN = W.

Le Tableau 4.1 résume les différents niveaux des facteurs.

Tableau 4.1 Niveaux des facteurs pour les mécanismes proposés

Facteurs	Niveaux des facteurs		
P_{Home}	0.6	0.75	0.9
$P_{VPLMNAd}$	0.3	0.5	0.75
$P_{HPLMNAP}$	0.6	0.8	1
P[Liste | VPLMNAd]=X	0.5	0.7	0.99
P[VPLMNAP | VPLMNAd]=Y	0.5	0.7	0.99
$P[VPLMNAP \mid VPLMNAd]_{APN}$ =Z	0.65		
$P_{APN\text{-}OI}$	0.85		
P_{DNS}	0.45		
P[HAPN-OI | APN-OI] = W	0.75		
$P_{APNSGSN}$	0.8		

Actuellement, on estime qu'environ 10% des usagers d'un réseau donné se trouvent en *roaming*. Aussi, nous faisons varier le facteur P_{Home} de 0.9 à 0.6 en passant par 0.75. La valeur de 0.9 représente la situation actuelle tandis que les deux autres valeurs correspondent à une situation future possible où le quart des usagers sont en *roaming* et une situation utopique où presque la moitié des usagers sont en dehors de leur réseau.

De la même façon, on estime que seulement 30 à 50% du trafic généré par les usager en *roaming* est traité par un GGSN local [25]. Pourquoi ? Parce que l'occurrence de la combinaison de paramètres nécessaires pour que se déroule ce scénario n'est pas favorisée. En effet, pour arriver au scénario dans lequel l'usager dans un réseau visité est servi par un GGSN local, il faut au moins que l'usager

possède un *Access Point Name* qui fait référence à un GGSN local. Présentement, cette seule condition n'est remplie que par une minorité des usagers en *roaming*. C'est également sur ce point que se distingue le *ServiceID*. Techniquement, ce dernier fait aussi bien référence à un GGSN local qu'à un GGSN dans le réseau d'origine de l'usager. La condition précédemment citée est donc toujours remplie. Par ailleurs, nous formulons également les hypothèses suivantes :

- Les réseaux d'origine et visité ont des accords autorisant leurs usagers respectifs à utiliser les services de son pair ;
- Les réseaux possédant des accords de *roaming* possèdent au moins un GGSN capable de donner accès à chacun des services de son pair.

Ces deux hypothèses favorisent encore davantage l'occurrence du scénario désiré car elles assurent que les autres conditions nécessaires à son déroulement sont remplies :

- La première garantit que l'usager possède l'autorisation d'utiliser les services d'un GGSN local (facteur $P_{VPLMNAd}$) ainsi que l'accès au point d'accès du réseau visité (facteur Y) ;
- La seconde certifie que si la première hypothèse est satisfaite alors le *ServiceID* du service requis par l'usager est obligatoirement présent dans la liste de GGSNs du réseau visité (facteur X).

En d'autres termes, ces hypothèses augmentent les valeurs des différents facteurs. Les choix des niveaux de $P_{VPLMNAd}$, X et Y a été fait pour représenter la situation actuelle (valeurs basses) et la situation souhaitée (valeurs hautes). Il nous est difficile d'établir avec précision à quel point les mécanismes proposés et nos hypothèses affectent les facteurs. Cependant, on peut raisonnablement affirmer que les valeurs recherchées sont bornées par celles des situations présente et utopique.

Parmi les facteurs spécifiques au système basé sur l'APN, $P_{APN\text{-}OI}$ et P[HAPN-OI | APN-OI] ont des valeurs constantes car ce n'est pas le système

actuel qui nous intéresse. Nous avons uniquement besoin de savoir comment le système actuel réagit pour pouvoir le comparer à notre solution.

Tableau 4.2 Plan d'expérience

	P_{Home}	$P_{VPLMNAd}$	$P_{HPLMNAP}$	X	Y
Session 1	0.6	0.75	0.8	0.99	0.99
Session 2	0.75	0.75	0.8	0.99	0.99
Session 3	0.9	0.75	0.8	0.99	0.99
Session 4	0.75	0.3	0.8	0.99	0.99
Session 5	0.75	0.5	0.8	0.99	0.99
Session 6	0.75	0.75	0.8	0.99	0.99
Session 7	0.75	0.75	0.6	0.99	0.99
Session 8	0.75	0.75	1	0.99	0.99
Session 9	0.9	0.5	0.8	0.5	0.7
Session 10	0.9	0.5	0.8	0.7	0.7
Session 11	0.9	0.5	0.8	0.99	0.7
Session 12	0.9	0.75	0.8	0.99	0.5
Session 13	0.9	0.75	0.8	0.99	0.7

Nous avons déterminé les facteurs et leurs niveaux. À présent, il nous reste à définir le type d'expérience que nous désirons mener. Nous avons le choix entre les types suivants : factoriel, aléatoire, un facteur à la fois. Une expérience factorielle comprend toutes les combinaisons possibles des niveaux de facteurs. Dans notre cas, cela correspondrait à $3^5 = 243$ sessions différentes à exécuter. Ce nombre de sessions est prohibitif d'autant plus que certaines d'entre elles sont redondantes du point de vue des informations qu'elles apportent. Une expérience aléatoire, comme son nom l'indique, choisit au hasard les sessions à inclure dans l'expérience. Ce type d'expérience pourrait nous faire passer à côté de résultats intéressants. Enfin, le

dernier type d'expérience, un facteur à la fois, consiste à faire varier un facteur à la fois tandis que les autres restent constants. Il permet de mettre en évidence l'influence de chaque facteur. C'est ce dernier que nous avons choisi d'expérimenter.

L'étape suivante de notre évaluation consiste à établir notre plan d'expérience. Ce dernier est présenté au Tableau 4.2.

Le type d'expérience choisi est un facteur à la fois. Aussi, l'influence de chaque facteur est étudié à l'aide de trois sessions. Le choix des valeurs constantes des autres facteurs est important puisqu'il définit le contexte.

Tableau 4.3 Résultats de l'expérience

	Délai Moyen	Temps exécution	Pourcentage réussite	(Délai Moyen)$_{APN}$	(Temps exécution)$_{APN}$	(Pourcentage réussite)$_{APN}$
Session1	167,961494	256,803552	0,978806	175,2727081	288,6974925	0,999723125
Session2	168,350934	252,00222	0,98675375	170,2270051	268,0471828	0,983889453
Session3	168,740374	247,200888	0,9947015	165,181302	247,3968731	0,968055781
Session4	167,270374	265,320888	0,9647015	149,565177	232,1883731	0,867930781
Session5	167,750623	259,40148	0,9745025	158,7482117	248,1256219	0,919467969
Session6	168,350934	252,00223	0,98675375	170,2270051	268,0471828	0,983889453
Session7	165,71493	245,961559	0,9735075	167,0119113	260,6799328	0,967733203
Session8	170,986938	258,042881	1	173,4420988	275,4144328	1
Session9	168,1915	253,98	0,9835	160,5897847	239,4282488	0,942287188
Session10	168,2601	253,1288	0,9849	160,5897847	239,4282488	0,942287188
Session11	168,35957	251,89456	0,98693	160,5897847	239,4282488	0,942287188
Session12	168,383825	251,5956	0,987425	165,181302	247,3968731	0,968055781
Session13	168,529355	249,80184	0,990395	158,590302	237,8808731	0,929055781

4.3.3 Résultats

Cette sous-section est consacrée à la présentation et à la discussion des résultats de l'expérience. Le Tableau 4.3 expose les résultats de l'expérience.

Nous allons analyser ces résultats indice par indice en commençant par le délai moyen de la communication de l'usager. Cependant, l'appréciation générale que nous avons en regardant les résultats dans leur ensemble est que les facteurs influencent grandement les conclusions de la comparaison entre les deux systèmes étudiés. Les performances de ces derniers sont donc sensibles au contexte dans lequel ils sont exécutés.

L'étude des sessions 1, 2 et 3 ainsi que la Figure 4.8, nous permet de déduire que l'efficacité des mécanismes d'abolition de l'ancrage géographique de l'APN est subordonnée au pourcentage des usagers qui visitent un réseau étranger. Plus il y a d'usagers en *roaming*, plus notre solution se révèle efficace par rapport au système actuel basé sur l'APN.

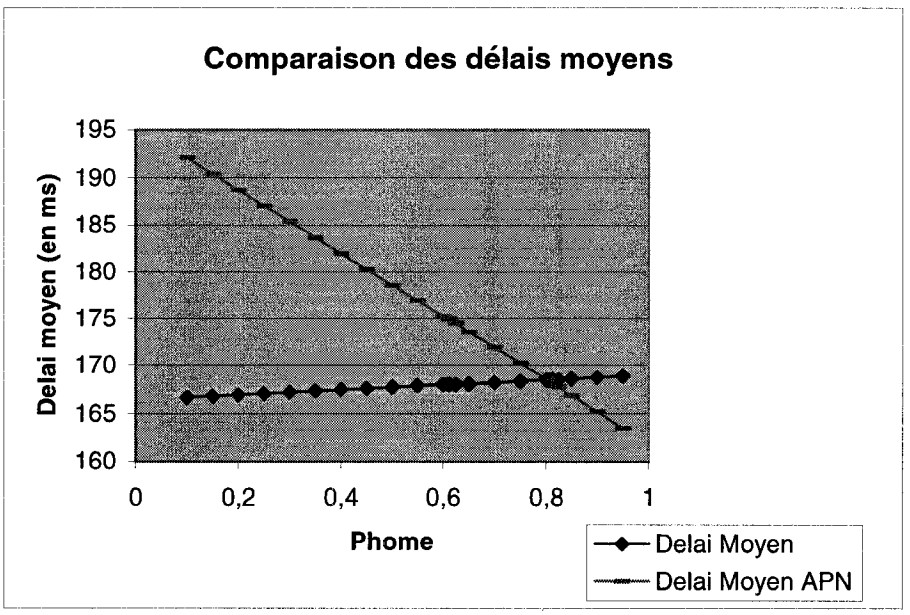


Figure 4.8 Comparaison des délais moyens soulignant l'importance du nombre d'usagers en roaming

De la même manière, les sessions 4, 5 et 6 soulignent l'importance de la première hypothèse que nous avons posée pour favoriser l'occurrence du scénario 2 : les réseaux d'origine et visité ont des accords autorisant leurs usagers respectifs à

utiliser les services de son pair. Ainsi, le mécanisme d'abolition de l'ancrage de l'APN a besoin pour performer qu'un nombre conséquent de réseaux possèdent des accords de *roaming*. Sans cela, le délai moyen subi par le trafic de l'usager dans le système actuel basé sur l'APN est inférieur à celui de notre solution comme le montre la Figure 4.9.

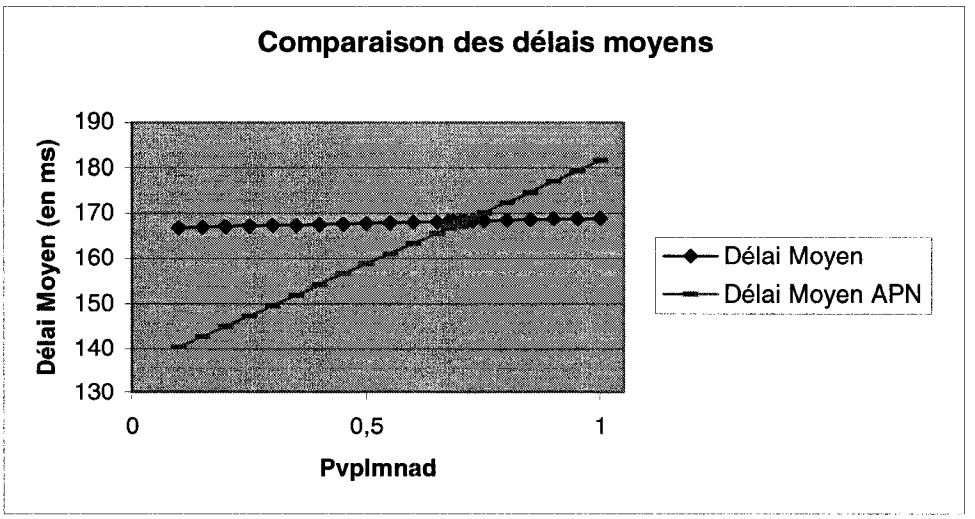


Figure 4.9 Comparaison des délais moyens soulignant l'importance des accords de roaming

Les sessions 6, 7 et 8, en revanche, révèlent que le facteur $P_{HPLMNAP}$ n'a pas d'effet significatif sur le délai moyen des communication de l'usager dans le contexte de notre analyse.

Les sessions 9, 10 et 11 ont été conçues pour étudier l'importance de la seconde hypothèse que nous avons posée : les réseaux possédant des accords de *roaming* possèdent au moins un GGSN capable de donner accès à chacun des services de son pair. On peut voir que si la première hypothèse n'est pas satisfaite, la seconde n'a aucun effet sur la performance de notre solution qui se révèle alors inférieure à celle du système actuel.

En ce qui concerne le second indice de performance, le temps d'exécution des mécanismes, l'analyse de l'ensemble des sessions met clairement en évidence l'importance du facteur P_{Home} qui détermine quel mécanisme est plus performant que l'autre. Encore une fois, un pourcentage d'usager en *roaming* supérieur à 25% est nécessaire pour que notre solution soit la plus performante. Les sessions 4, 5 et 6 et la Figure 4.10 soulignent également l'importance des deux hypothèses que nous avons émises sur les accords de *roaming*.

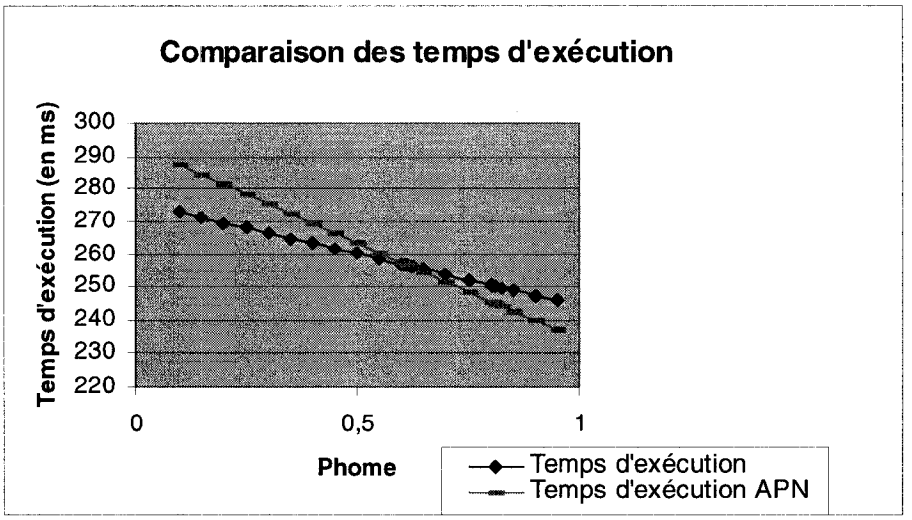


Figure 4.10 Comparaison des temps d'exécution soulignant l'importance du nombre d'usagers en roaming

Enfin, le dernier indice de performance, soit le pourcentage de réussite des mécanismes, démontre clairement que notre solution diminue l'occurrence des cas d'échec de la procédure d'activation de PDP *Context*. En d'autres termes, plus de requêtes sont traitées avec succès par notre mécanisme quels que soient les niveaux des facteurs.

Ainsi s'achève notre analyse de performance. Nous avons pu établir que nos mécanismes visant à abolir l'ancrage géographique de l'APN permettent effectivement de réduire les délais liés à ce problème. Nous avons donc atteint

l'objectif principal de ce travail. Nous devons cependant souligner l'importance du pourcentage d'usager en *roaming* ainsi que du nombre de réseaux partageant des accords de *roaming*. Ce sont en effet des valeurs élevées de ces facteurs qui garantissent une performance élevée de notre solution.

CHAPITRE 5
CONCLUSION

Ce mémoire a essentiellement traité de l'ancrage géographique de l'*Access Point Name* et de son abolition pour une meilleure qualité de service dans les réseaux UMTS. Le présent chapitre résume l'ensemble des travaux et contributions, en signale les limitations et propose de nouvelles pistes de recherche et améliorations.

5.1 Synthèse des travaux

Ce mémoire a traité d'un problème crucial pour la qualité de service ainsi que pour la gestion de la mobilité dans les réseaux UMTS. Nous avons proposé un nouveau mécanisme capable d'abolir l'ancrage géographique de *l'Access Point Name* lorsqu'un usager est en visite dans un réseau étranger. Le succès de ce mécanisme repose sur deux éléments. Le premier est son principe de base : contrairement à l'*Access Point Name*, le "*ServiceID*" désigne un réseau de données ou un service et laisse au réseau dans lequel se trouve l'usager le soin de choisir le GGSN capable de le servir. Les hypothèses énoncées constituent le second élément et elles garantissent les conditions nécessaires pour qu'un usager en *roaming* soit servi pour un GGSN du réseau visité. Notre mécanisme a donc besoin d'accords de *roaming* entre les réseaux d'origine et visité impliquant que chaque réseau possède au moins un GGSN capable de fournir chaque service de son pair.

Le mécanisme d'abolition de l'ancrage géographique de l'*Access Point Name* a été modélisé grâce au logiciel de vérification formelle UPPAAL. Nous avons ainsi pu valider les propriétés de notre mécanisme en ce qui a trait à sa manière de réagir face à certaines situations indésirables ou non, à sa survivabilité et à son intégrité. D'un point de vue formel, le mécanisme possède le comportement que nous souhaitions.

Une analyse de performance a permis de mettre en évidence les performances de notre solution. Ainsi, cette dernière atteint bel et bien notre objectif principal : réduire les délais liés à l'ancrage géographique de l'APN lorsque l'usager est en *roaming*. Nous avons également déterminé que cette performance est fortement reliée au nombre d'usagers en *roaming* et au nombre de réseaux qui partagent des accords de *roaming*. Il est nécessaire que ces deux derniers nombres soient élevés pour garantir que notre mécanise performe mieux que le système actuel basé sur l'APN.

5.2 Limitations des travaux

La gestion de mobilité constituait l'une des facettes du problème qui nous a intéressé dans ce mémoire. Or, cette dernière est le plus souvent associée à la résolution des problèmes de *handover* ou de relève. Une relève est l'ensemble des techniques utilisées pour permettre à un usager mobile de passer d'une cellule à une autre sans que la communication ne soit interrompue. Dans ce mémoire, nous avons pu éviter de traiter de relève grâce à l'une de nos hypothèses de départ : cette dernière stipule que nous ne considérons que les cas de mobilité sans relève. Puisque notre travail adresse les scénarii de déplacements intercontinentaux, il est logique de supposer qu'en aucune façon, un usager maintiendra une communication de plusieurs heures durant son voyage jusqu'à destination. Cependant, la solution proposée peut également être utilisée lors de déplacements entre des réseaux moins éloignés géographiquement. Il serait alors intéressant d'analyser comment notre mécanisme d'abolition de l'ancrage géographique de l'*Access Point Name* influence la relève et éventuellement, dans quelle mesure, notre solution peut être améliorée.

Par ailleurs, l'une des limitations majeures de notre mécanisme réside dans le fait qu'il ne peut être introduit progressivement. En effet, l'utilisation du *ServiceID* et de l'*Access Point Name* s'exclue complètement. Cela constitue une barrière assez importante à la propagation de notre mécanisme puisqu'il n'est pas interopérable.

Enfin, la procédure de découverte de l'adresse IP du HGGSN suppose qu'il existe une adresse IP permettant de rejoindre tous les SGSNs d'un réseau donné. Ce type d'adresse n'a pas encore été défini. Il en va de même de la procédure qui permettrait de choisir parmi tous les SGSNs d'un réseau celui qui traitera la requête du message *ICMP Home GGSN Address Discovery Request.*

5.3 Indication de travaux futurs

Cette sous-section avec laquelle nous allons clore ce mémoire présente d'éventuelles pistes de recherche. Ces dernières découlent des différentes limitations de la solution proposée et sont une invitation à l'améliorer.

Une première piste serait donc de traiter le problème de l'ancrage géographique de l'*Access Point Name* mais en considérant les cas avec relève dans la continuité de notre travail.

Une seconde piste et selon nous, la plus cruciale, concerne l'inter-opérabilité de notre mécanisme avec le système actuel basé sur l'*Access Point Name.* Elle permettrait une introduction progressive de notre mécanisme dans les différents réseaux UMTS et le rendrait plus attrayant.

BIBLIOGRAPHIE

[1] The 3rd Generation Partnership Project. 2005. "General Packet Radio Service (GPRS); Service description; Stage 2". Release 5. TS 23.060 version 5.10.0, 208 pages.

[2] The 3rd Generation Partnership Project. 2002. "Numbering, addressing and identification". Release 1999. TS 23.003 version 3.10.0, 34 pages.

[3] The 3rd Generation Partnership Project. 2002. "QoS concept and Architecture". Release 5. TS 23.107 version 5.5.0, 40 pages.

[4] Semeria, C., "BGP/MPLS VPN Fundamentals". RFC 2547bis. 2001.

[5] Rosen, E., Wismanathan, A., Callon, R., "Multiprotocol Label Swithing architecture". RFC 3031. Janvier 2001.

[6] Deering, S., Hinden, R., "Internet Protocol, version 6 (Ipv6) Specification". RFC 2460. Décembre 1998.

[7] Johnson, D., Perkins, C., Arkko, J., "Mobility support in IPv6". RFC 3775. Juin 2004.

[8] Narten, T., Nordmark, E., Simpson, W., "Neighbor discovery for IP version 6 (IPv6) ". RFC 2461. Décembre 1998.

[9] Davie, Bruce, Rekhter, Yakov., 2000. "MPLS technology and applications". Morgan Kaufmann Publishers, 2000.

[10] Tatipamula, M., Grossetete, P., Esaki, H., 2004. "IPv6 integration and coexistence strategies for next-generation networks". *IEEE Communications Magazine*, vol. 42, no. 1, pp. 88 – 96.

[11] Roesler, V., Balbinot, L., De Andrade, M., Tarouco, L., 2002. "IP next generation label switching". 2002. *IEEE Workshop on IP Operations and Management*, pp. 21 – 25.

[12] Uda, S., Ogashiwa, N., Uo, Y., Hinoda, Y., 2003. "IPv6 support on MPLS networks: experiences with 6PE approach". *Symposium on applications and the Internet Workshops Proceedings 2003*, pp. 226 – 231.

[13] Tingzhou, Y., Yixin, D., Bin, Z., Makrakis, D., 2002. "Profile-based mobile MPLS protocol". 2002. *IEEE CCECE Canadian Conference on Electrical and Computer Engineering.* 3, pp. 1352 – 1356.

[14] Chiussi, F.M., Khotimsky, D.A., Krishnan, S., 2003. " Mobility management in third-generation all-IP networks". *IEEE Communications Magazine.* vol. 40, no. 9, pp. 124 – 135.

[15] Roos, A., Hartman, M., Dutnall, S., 2003. "Critical issues for roaming in 3G". *IEEE Wireless Communications Magazine.* vol. 10, no. 1, pp. 29 – 35.

[16] Brandolini, M., Rossi, P., Manstretta, D., Svelto, F., 2005. "Toward multistandard mobile terminals - fully integrated receivers requirements and architectures". *IEEE Transaction on Microwave Theory and Techniques.* vol. 53, no. 3, part 2, pp. 1026 – 1038.

[17] Yi-Bin, L., Ming-Feng, C., Meng-Ta, H., Lin-Yi, W., 2005. "One-pass GPRS and IMS authentication procedure for UMTS". *IEEE Journal on Selected Areas in*

Communications. vol. 23, no. 6, pp. 1233 – 1239.

[18] Huber, J.F., 2004. "Mobile next-generation networks". *IEEE Multimedia.* vol. 11, no. 1, pp. 72 – 83.

[19] Ali, R.B., Pierre, S., Lemieux, Y., 2005. "UMTS-to-IP QoS mapping for voice and video telephony services". *IEEE Network.* vol. 19, no. 2, pp. 26 – 32.

[20] Daugherty, B., Metz, C., 2005. "Multiprotocol label switching and IP. Part I. MPLS VPNs over IP tunnels". *IEEE Internet Computing.* vol. 9, no. 3, pp. 68 – 72.

[21] Luyuang, Fang., Bita, N., Le Roux, J.-L., Miles, J., 2005. "Interprovider IP-MPLS services: requirements, implementations, and challenges". *IEEE Communications Magazine.* vol. 43, no. 6, pp. 119 – 128.

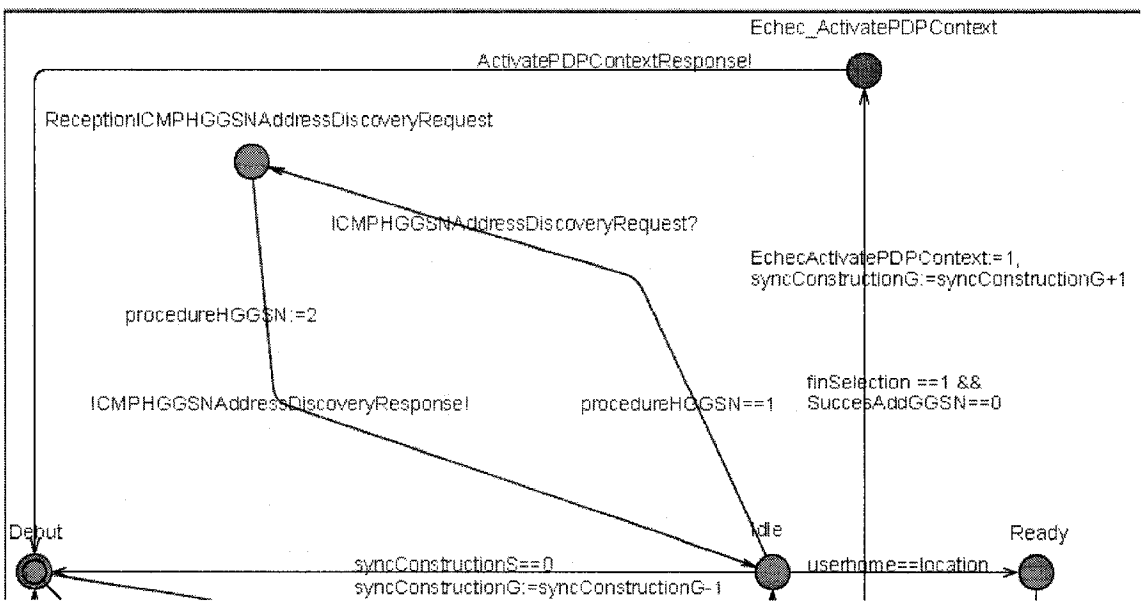
[22] Tatipamula, M., Grossetete, P., Esaki, H., 2004. "IPv6 integration and coexistence strategies for next-generation networks". *IEEE Communications Magazine.* vol. 42, no. 1, pp. 88 – 96.

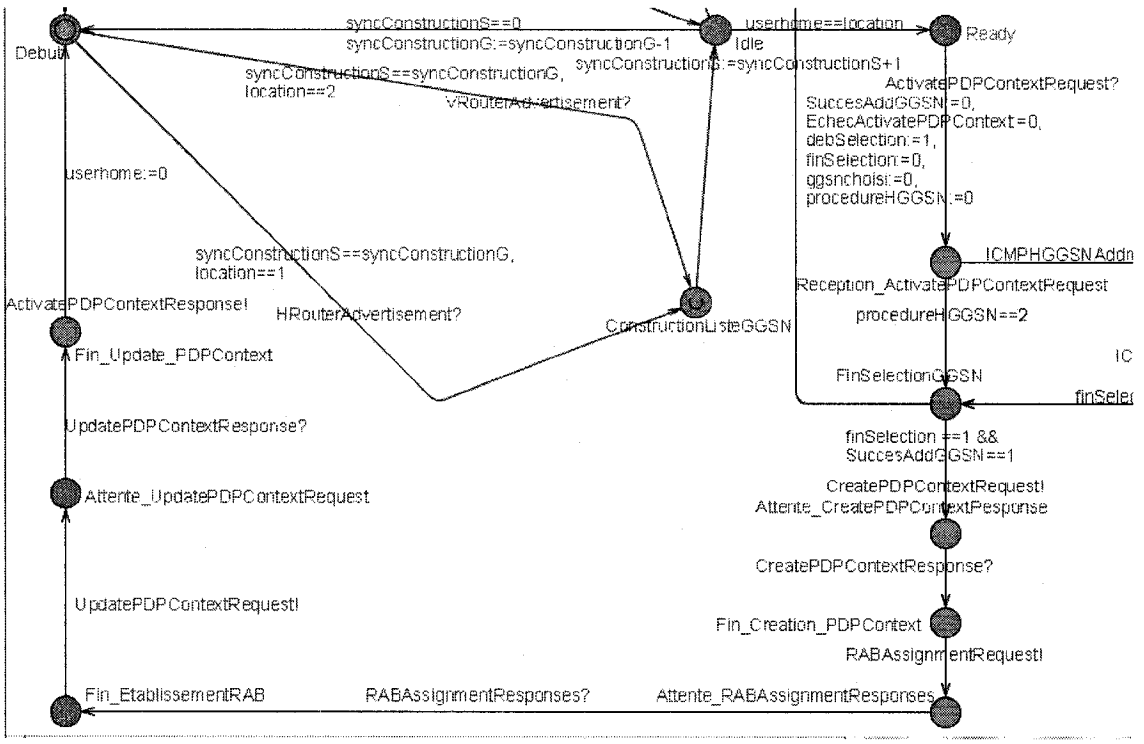
[23] Jie, L., Hsiao-Hwa, C., 2005. "Mobility support for IP-Based networks". *IEEE Communications Magazine.* vol. 43, no. 10, pp. 127 – 132.

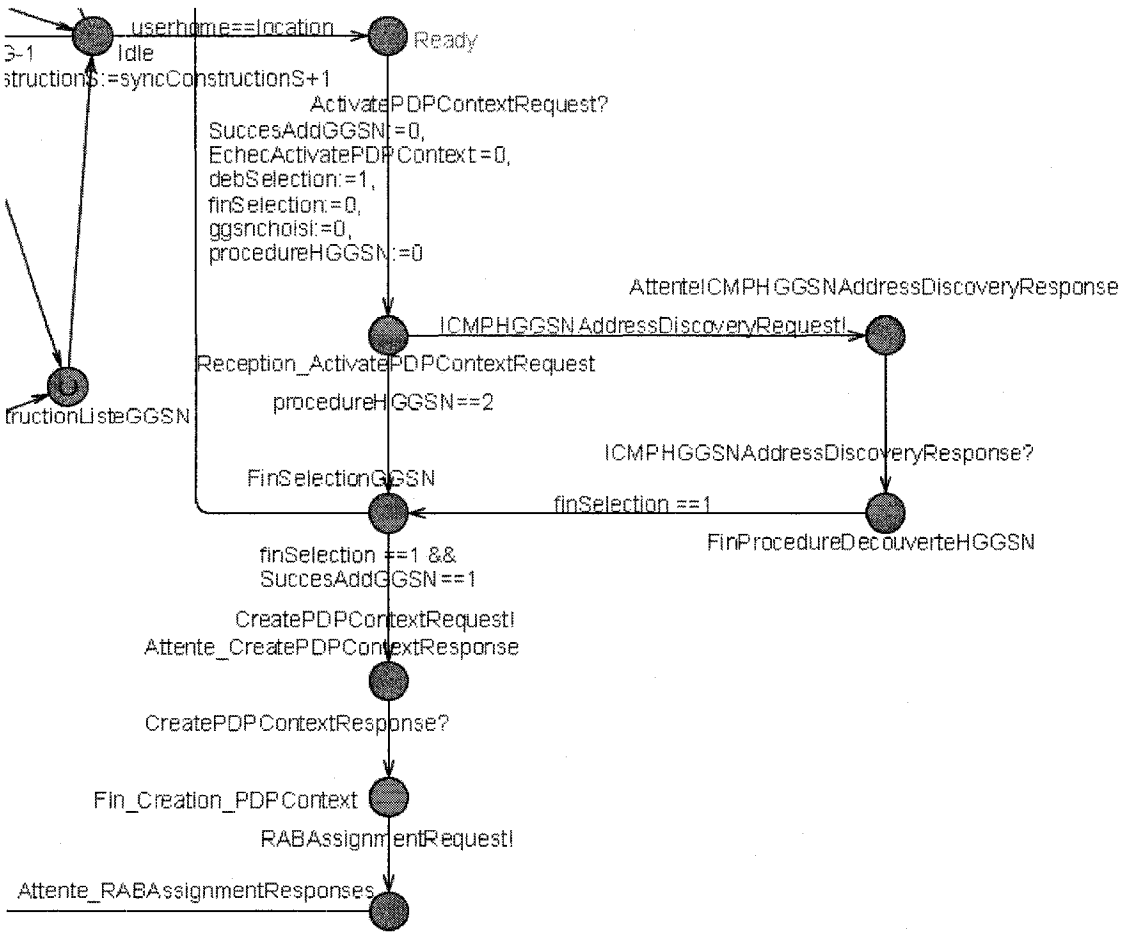
[24] Lemieux, Y., 2005. "Evolution du protocole GTP dans un contexte de VPN et mobilite-IP". Mémoire de maîtrise en génie informatique, École Polytechnique de Montréal.

[25] Lemieux, Yves. 2005. "Next generation IPv6 Test-bed plan". version 3. Document d'entreprise.

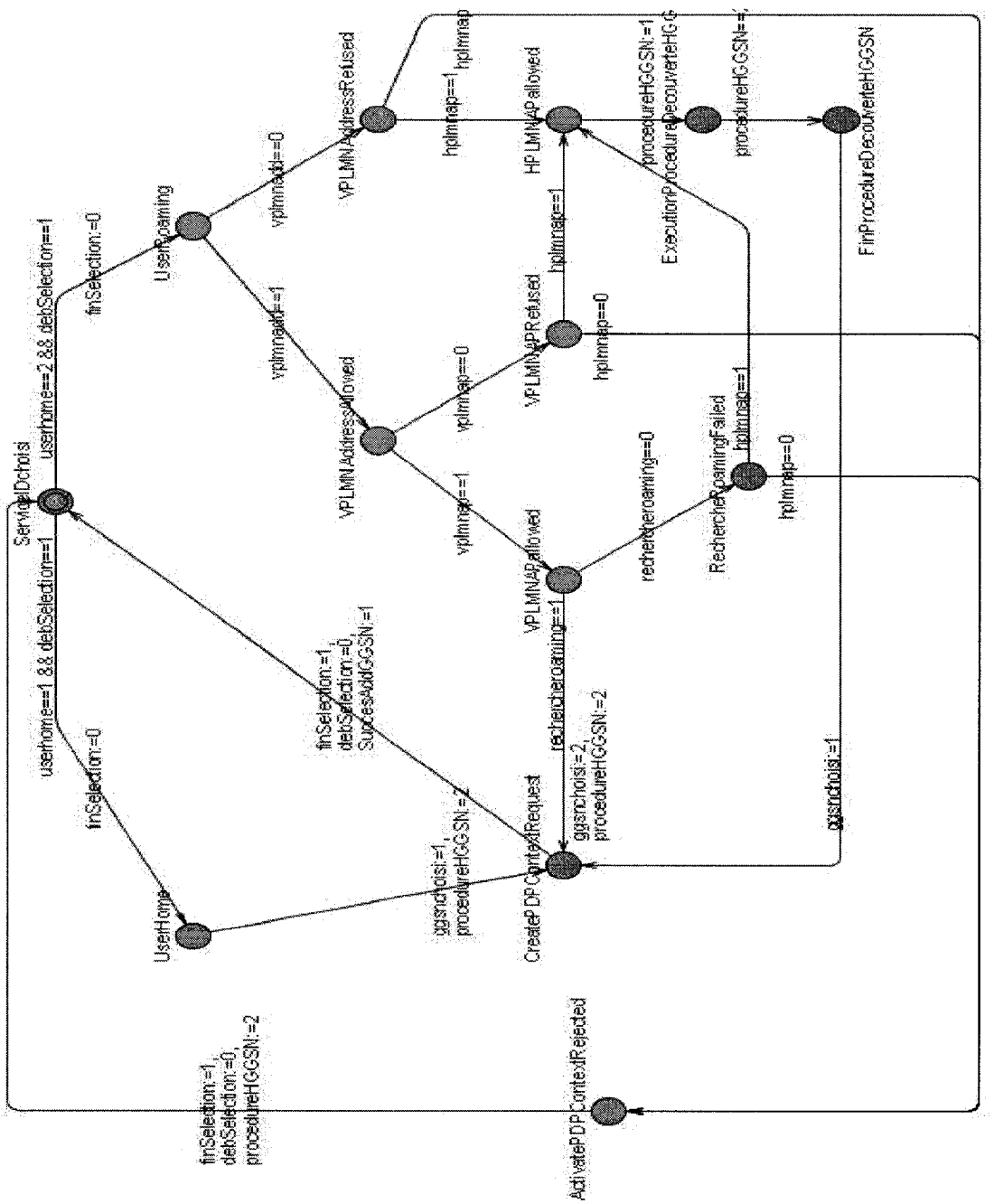
ANNEXE 1
AUTOMATE DU SGSN




syncConstructionS==0
syncConstructionG:=syncConstructionG-1
Debut
Idle
userhome==location
Ready
syncConstructionS:=syncConstructionS+1
ActivatePDPContextRequest?
SuccesAddGGSN:=0,
EchecActivatePDPContext:=0,
debSelection:=1,
finSelection:=0,
ggsnchoisi:=0,
procedureHGGSN:=0
syncConstructionS==syncConstructionG,
location==2
vRouterAdvertisement?
userhome:=0
syncConstructionS==syncConstructionG,
location==1
ICMPHGGSNAddn
Reception_ActivatePDPContextRequest
procedureHGGSN==2
ActivatePDPContextResponse!
HRouterAdvertisement?
ConstructionListeGGSN
Fin_Update_PDPContext
FinSelectionGGSN
finSelec
UpdatePDPContextResponse?
finSelection ==1 &&
SuccesAddGGSN==1
CreatePDPContextRequest!
Attente_UpdatePDPContextRequest
Attente_CreatePDPContextResponse
CreatePDPContextResponse?
UpdatePDPContextRequest!
Fin_Creation_PDPContext
RABAssignmentRequest!
Fin_EtablissementRAB
RABAssignmentResponses?
Attente_RABAssignmentResponses


userhome==location
Ready
Idle
ActivatePDPContextRequest?
SuccesAddGGSN:=0,
EchecActivatePDPContext:=0,
debSelection:=1,
finSelection:=0,
ggsnchoisi:=0,
procedureHGGSN:=0
AttenteICMPHGGSNAddressDiscoveryResponse
ICMPHGGSNAddressDiscoveryRequest!
Reception_ActivatePDPContextRequest
procedureHGGSN==2
ICMPHGGSNAddressDiscoveryResponse?
FinSelectionGGSN
finSelection ==1
FinProcedureDecouverteHGGSN
finSelection ==1 &&
SuccesAddGGSN==1
CreatePDPContextRequest!
Attente_CreatePDPContextResponse
CreatePDPContextResponse?
Fin_Creation_PDPContext
RABAssignmentRequest!
Attente_RABAssignmentResponse

ANNEXE 2
AUTOMATE DE SELECTIONGGSN



ANNEXE 3
PARAMÈTRES ET PLAN D'EXPÉRIENCE POUR L'APN

$(P_1)_{APN}$ = P[(Home ∩ !APN-OI) U (Home ∩ APN-OI ∩ HAPN-OI) U (Home ∩ APN-OI ∩ VAPN-OI ∩ APNSGSN)]

Hypothèses :

- La probabilité $(P_1)_{APN}$ est celle de la réunion de trois événements incompatibles (1) ;
- Tous les événements sont indépendants deux à deux excepté les paires d'événements APN-OI et VAPN-OI ainsi que VPLMNAd et VPLMNAP (2) ;
- P[HAPN-OI | APN-OI] = W (3) ;
- P[VAPN-OI] = 1-P[HAPN-OI] (4) ;

(1) → $(P_1)_{APN}$ = P[Home ∩ !APN-OI] + P[Home ∩ APN-OI ∩ HAPN-OI] + P[Home ∩ APN-OI ∩ VAPN-OI ∩ APNSGSN] ; (*)

(*) et (2) → $(P_1)_{APN}$ = P[Home]*P[!APN-OI] + P[Home]*P[APN-OI ∩ HAPN-OI] + P[Home]* P[APN-OI ∩ VAPN-OI]*P[APNSGSN] ; (**)

(3) → P[HAPN-OI ∩ APN-OI] = W*P_{APN-OI} ; (***)

(2) et (4) → P[VAPN-OI | APN-OI] = 1-W ; (****)

(****) → P[VAPN-OI ∩ APN-OI] = (1-W)*P_{APN-OI} ; (*****)

(**), (***) et (*****) → $(P_1)_{APN}$ = P_{Home}*(1-P_{APN-OI}) + P_{Home}* W*P_{APN-OI} + P_{Home}*(1-W)*P_{APN-OI} *$P_{APNSGSN}$;

$$\mathbf{(P_1)_{APN} = P_{Home}\,(1 + (W-1)*P_{APN\text{-}OI} + (1-W)*P_{APN\text{-}OI}*P_{APNSGSN})}$$

$(P_2)_{APN}$ = P[(!Home ∩ APN-OI ∩ VAPN-OI ∩ VPLMNAd ∩ VPLMNAP)
U (!Home ∩ APN-OI ∩ HAPN-OI ∩ VPLMNAd ∩ VPLMNAP ∩ APNSGSN)
U (!Home ∩ !APN-OI ∩ VPLMNAd ∩ VPLMNAP ∩ APNSGSN)
U (!Home ∩ !APN-OI ∩ VPLMNAd ∩ VPLMNAP ∩ !APNSGSN ∩ DNS)
U (!Home ∩ APN-OI ∩ HAPN-OI ∩ VPLMNAd ∩ VPLMNAP ∩ !APNSGSN ∩ DNS)]

Hypothèses :

- La probabilité $(P_2)_{APN}$ est celle de la réunion de cinq événements incompatibles (5) ;
- P[VPLMNAP | VPLMNAd] = Z (6) ;

(2) et (5) → $(P_2)_{APN}$ = P[!Home]*P[APN-OI ∩ VAPN-OI]*P[VPLMNAd ∩ VPLMNAP] + P[!Home]*P[APN-OI ∩ HAPN-OI]*P[VPLMNAd ∩ VPLMNAP]*P[APNSGSN)] + P[!Home]*P[!APN-OI]*P[VPLMNAd ∩ VPLMNAP]*P[APNSGSN)] + P[!Home]*P[!APN-OI]*P[VPLMNAd ∩ VPLMNAP]*P[!APNSGSN]*P[DNS] + P[!Home]*P[APN-OI ∩ HAPN-OI]*P[PLMNAd ∩ VPLMNAP] *P[!APNSGSN]*P[DNS] ; (#)

(6) → $P[VPLMNAP \cap VPLMNAd] = Z*P_{VLMNAd}$; (##)

(#), (##), (***) et (*****) → $(P_2)_{APN} = (1-P_{Home})*(1-W)*P_{APN-OI}*Z*P_{VLMNAd}$
$+ (1-P_{Home})*W*P_{APN-OI}*Z*P_{VLMNAd}*P_{APNSGSN}$
$+ (1-P_{Home})*(1-P_{APN-OI})*Z*P_{VLMNAd}*P_{APNSGSN}$
$+ (1-P_{Home})*(1-P_{APN-OI})*Z*P_{VLMNAd}*(1-P_{APNSGSN})*P_{DNS}$
$+ (1-P_{Home})*W*P_{APN-OI}*Z*P_{VLMNAd}*(1-P_{APNSGSN})*P_{DNS}$;

$$\mathbf{(P_2)_{APN} = (1-P_{Home}) *Z*P_{VLMNAd} *[((1-W)+ (W-1)*P_{DNS})*P_{APN-OI} + ((W-1)+(1-W)*P_{DNS})*P_{APN-OI}*P_{APNSGSN} + P_{APNSGSN} + P_{DNS} - P_{APNSGSN}*P_{DNS}] ;}$$

$(P_3)_{APN}$ = P[(!Home ∩ !APN-OI ∩ !VPLMNAd ∩ HPLMNAP) U (!Home ∩ !APN-OI ∩ VPLMNAd ∩ !VPLMNAP ∩ HPLMNAP) U (!Home ∩ APN-OI ∩ HAPN-OI ∩ HPLMNAP)]

Hypothèses :

- La probabilité $(P_3)_{APN}$ est celle de la réunion de trois événements incompatibles (7) ;

(7) → $(P_3)_{APN}$ = P[(!Home ∩ !APN-OI ∩ !VPLMNAd ∩ HPLMNAP)] + P[!Home ∩ !APN-OI ∩ VPLMNAd ∩ !VPLMNAP ∩ HPLMNAP] + P[!Home ∩ APN-OI ∩ HAPN-OI ∩ HPLMNAP] ; ($)

(2) → $(P_3)_{APN}$ = P[!Home]*P[!APN-OI]*P[!VPLMNAd]*[HPLMNAP] + P[!Home]*P[!APN-OI]*P[VPLMNAd ∩ !VPLMNAP]*P[HPLMNAP] + P[!Home]*P[APN-OI ∩ HAPN-OI]*P[HPLMNAP] ; ($$)

($$), (##) et (***) → $(P_3)_{APN} = (1-P_{Home})*(1-P_{APN-OI})*(1-P_{VPLMNAd})*P_{HPLMNAP} + (1-P_{Home})*(1-P_{APN-OI})*Z*P_{VLMNAd}*P_{HPLMNAP} + (1-P_{Home})*(1-W)*P_{APN-OI}*P_{HPLMNAP}$;

$$\mathbf{(P_3)_{APN} = (1-P_{Home}) * P_{HPLMNAP} * [(1-P_{APN-OI})*(1-P_{VPLMNAd}) + (1-P_{APN-OI})*Z*P_{VLMNAd} + (1-W)*P_{APN-OI}]}$$

$(P_4)_{APN}$ = P[(!Home ∩ VPLMNAd ∩ VPLMNAP ∩ !DNS)

(2) → $(P_4)_{APN}$ = P[!Home]* P[VPLMNAd ∩ VPLMNAP]*P[!DNS] ; (&)

(&),(##) → $(P_4)_{APN} = (1-P_{Home})*Z*P_{VLMNAd}*(1-P_{DNS})$;

$$\mathbf{(P_4)_{APN} = (1-P_{Home})*Z*P_{VLMNAd}*(1-P_{DNS})}$$

$(T_1)_{APN} = (T_2)_{APN} = 2*T_{ActivateMsg} + T_{Mécanisme} + 2*T_{DNSMsg} + 2*(T_{CreateMsg})_{1Réseau} + T_{CreateProcess} + T_{PorteuseRadio} + 2*(T_{UpdateMsg})_{1Réseau} + T_{UpdateProcess}$

$= 2*54 + 1 + 2*4 + 2*4 + 1 + 109 + 2*4 + 1 = 244$ ms ;

$(T_3)_{APN} = 2*T_{ActivateMsg} + T_{Mécanisme} + 2*T_{DNSMsg} + 2*(T_{CreateMsg})_{2Réseau} + T_{CreateProcess} + T_{PorteuseRadio} + 2*(T_{UpdateMsg})_{2Réseau} + T_{UpdateProcess}$

$= 2*54 + 1 + 2*4 + 2*38 + 1 + 109 + 2*38 + 1 = 304$ ms ;

$(T_4)_{APN} = 2*T_{ActivateMsg} + T_{Mécanisme} + 4*T_{DNSMsg} + 2*(T_{CreateMsg})_{2Réseau} + T_{CreateProcess} + T_{PorteuseRadio} + 2*(T_{UpdateMsg})_{2Réseau} + T_{UpdateProcess}$

$= 2*54 + 1 + 4*4 + 2*38 + 1 + 109 + 2*38 + 1 = 312$ ms ;